(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2018-201235
(P2018-201235A)
(43)公開日　平成30年12月20日(2018.12.20)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/32	(2006.01)	H04L	9/00	675A	5J104
		H04L	9/00	675B	

審査請求 有　請求項の数 18　ＯＬ　（全 32 頁）

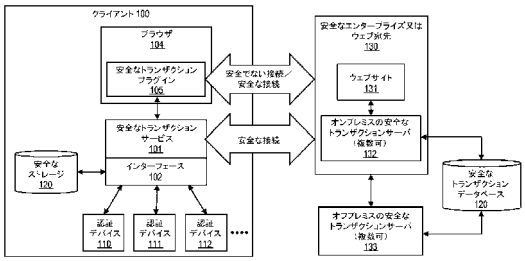
(21)出願番号	特願2018-153218 (P2018-153218)
(22)出願日	平成30年8月16日 (2018.8.16)
(62)分割の表示	特願2015-550778 (P2015-550778)の分割
原出願日	平成25年12月26日 (2013.12.26)
(31)優先権主張番号	13/730,761
(32)優先日	平成24年12月28日 (2012.12.28)
(33)優先権主張国	米国(US)
(31)優先権主張番号	13/730,776
(32)優先日	平成24年12月28日 (2012.12.28)
(33)優先権主張国	米国(US)
(31)優先権主張番号	13/730,780
(32)優先日	平成24年12月28日 (2012.12.28)
(33)優先権主張国	米国(US)

(71)出願人　514108090
ノック　ノック　ラブズ，　インコーポレイテッド
Ｎｏｋ　Ｎｏｋ　Ｌａｂｓ，　Ｉｎｃ．
アメリカ合衆国　カリフォルニア　９４３０３，　パロ　アルト，　ミドルフィールド　ロード　４１５１，　スイート　２００
４１５１　Ｍｉｄｄｌｅｆｉｅｌｄ　Ｒｏａｄ，　Ｓｕｉｔｅ　２００，　Ｐａｌｏ　Ａｌｔｏ，　ＣＡ　９４３０３　Ｕｎｉｔｅｄ　Ｓｔａｔｅｓ
(74)代理人　100092093
弁理士　辻居　幸一

最終頁に続く

(54)【発明の名称】認証能力を決定するためのクエリシステム及び方法

(57)【要約】　（修正有）
【課題】ネットワーク上での安全なユーザ認証を提供する。
【解決手段】Ｎ＞１である、クライアント１００上のＮ個の認証デバイス１１０、１１１、１１２を検出し、Ｎ個の認証デバイスの各々に１つずつ、Ｎ個の暗号エンティティを生成し、Ｎ個の暗号エンティティの各々をＮ個の認証デバイスの各々に登録するコマンドをクライアントに送信し、クライアント上でコマンドを実行し、それに応答してＮ個の暗号エンティティの各々をそれぞれのＮ個の認証デバイスの各々に登録し、その後、認証デバイス及びその関連付けられた暗号エンティティのうちの少なくとも１つを使用して、ネットワーク上でクライアントのユーザを認証する。
【選択図】図１Ａ



【特許請求の範囲】
【請求項１】
方法であって、
Ｎ＞１である、クライアント上のＮ個の認証デバイスを検出する工程と、
前記Ｎ個の認証デバイスの各々に１つずつ、Ｎ個の暗号エンティティを生成する工程と、
前記Ｎ個の暗号エンティティの各々を前記Ｎ個の認証デバイスの各々に登録するコマンドをサーバから前記クライアントに送信し、且つ第１のランダムチャレンジを前記サーバから前記クライアントに送信する工程と、
前記Ｎ個の認証デバイスの各々にそれぞれが対応するＮ個のプライバシークラスを決定する工程であって、前記プライバシークラスが、対応する認証デバイスに関連するクライアント情報がユーザ又はクライアントデバイスを一意的に識別しているリストに基づいて、決定される、前記工程と、
前記クライアント上で前記コマンドを実行し、それに応答して前記Ｎ個の暗号エンティティの各々を前記それぞれのＮ個の認証デバイスの各々に登録する工程と、
前記第１のランダムチャレンジに関連するタイムアウト期間に基づいて、前記第１のランダムチャレンジがもはや有効でないことを、前記クライアントにおいて自動的に検出する工程と、
これに応答して、前記クライアントから前記サーバへの新しいランダムチャレンジの要求を、ユーザの介在無しに、送信する工程と、
前記サーバで新しいランダムチャレンジを生成し、この新しいランダムチャレンジを前記クライアントに送信する工程と、
前記Ｎ個の認証デバイスの全てが登録されたという通知と共に前記新しいランダムチャレンジを前記サーバに戻し送信する工程であって、前記サーバが、受信された前記新しいランダムチャレンジが送信された前記新しいランダムチャレンジと同じであることを検証する工程と、
その後、前記認証デバイスの少なくとも一つ及びその関連付けられた暗号エンティティを使用して、ネットワーク上で前記クライアントのユーザを、前記サーバ又は異なるサーバで認証する工程と、を含み、前記クライアントのユーザを認証するために使用される前記認証デバイスの少なくとも一つがそれに対応するプライバシークラスに基づいている、方法。
【請求項２】
前記暗号エンティティが、鍵を含む、請求項１に記載の方法。
【請求項３】
前記鍵が、対称鍵を含み、所定の鍵の同一のコピーが、前記クライアント上の安全なストレージ、及びサーバと関連付けられた安全なストレージ内に記憶される、請求項２に記載の方法。
【請求項４】
前記鍵が、非対称鍵対を含み、前記鍵対の第１の鍵が、前記クライアント上の安全なストレージ内に記憶され、前記鍵対の第２の鍵が、サーバと関連付けられた安全なストレージ内に記憶される、請求項２に記載の方法。
【請求項５】
前記鍵が、鍵プロビジョニングプロトコルを使用して送信される、請求項２に記載の方法。
【請求項６】
前記鍵プロビジョニングプロトコルが、動的対称鍵プロビジョニングプロトコル（ＤＳＫＰＰ）を含む、請求項５記載の方法。
【請求項７】
ユーザを認証するために前記認証デバイスのうちの少なくとも１つ及びその関連付けられた暗号エンティティを使用する工程が、

前記認証デバイスから生体ユーザ入力を受信する工程と、
前記生体ユーザ入力が前記ユーザの認証に成功したことを決定する工程と、
前記認証デバイスと関連付けられた前記暗号エンティティを使用して、サーバに送信される情報を暗号化する工程と、を含む、請求項１に記載の方法。
【請求項８】
前記Ｎ個の認証デバイスが、生体認証デバイスを含み、
前記Ｎ個の暗号エンティティを前記Ｎ個の認証デバイス毎に一つずつ発生する前に、前記クライアント上の前記Ｎ個の認証デバイスで前記ユーザをエンロールすることを含む請求項１に記載の方法。
【請求項９】
前記サーバが、特定の認証デバイスと関連付けられた暗号エンティティを使用して、前記クライアント及び／又は前記認証デバイスの身元を検証する、請求項１に記載の方法。
【請求項１０】
プログラムコードを記憶するための少なくとも一つのメモリと、プログラムコードを処理するための少なくとも一つのプロセッサと、を含むシステムであり、前記プログラムコードの処理によって、
Ｎ＞１である、クライアント上のＮ個の認証デバイスを検出する手順と、
前記Ｎ個の認証デバイスの各々に１つずつ、Ｎ個の暗号エンティティを生成する手順と、
前記Ｎ個の暗号エンティティの各々を前記Ｎ個の認証デバイスの各々に登録するコマンドをサーバから前記クライアントに送信し、且つ第１のランダムチャレンジを前記サーバから前記クライアントに送信する手順と、
前記Ｎ個の認証デバイスの各々にそれぞれが対応するＮ個のプライバシークラスを決定する手順であって、前記プライバシークラスが、対応する認証デバイスに関連するクライアント情報がユーザ又はクライアントデバイスを一意的に識別しているリストに基づいて、決定される、前記手順と、
前記クライアント上で前記コマンドを実行し、それに応答して前記Ｎ個の暗号エンティティの各々を前記それぞれのＮ個の認証デバイスの各々に登録する手順と、
前記第１のランダムチャレンジに関連するタイムアウト期間に基づいて、前記第１のランダムチャレンジがもはや有効でないことを、前記クライアントにおいて自動的に検出する手順と、
これに応答して、前記クライアントから前記サーバへの新しいランダムチャレンジの要求を、ユーザの介在無しに、送信する手順と、
前記サーバで新しいランダムチャレンジを生成し、この新しいランダムチャレンジを前記クライアントに送信する手順と、
前記Ｎ個の認証デバイスの全てが登録されたという通知と共に前記新しいランダムチャレンジを前記サーバに戻し送信する手順であって、前記サーバが、受信された前記新しいランダムチャレンジが送信された前記新しいランダムチャレンジと同じであることを検証する手順と、
その後、前記認証デバイスの少なくとも一つ及びその関連付けられた暗号エンティティを使用して、ネットワーク上で前記クライアントのユーザを、前記サーバ又は異なるサーバで認証する手順と、が実行され、前記クライアントのユーザを認証するために使用される前記認証デバイスの少なくとも一つがそれに対応するプライバシークラスに基づいている、前記システム。
【請求項１１】
前記暗号エンティティが、鍵を含む、請求項１に記載のシステム。
【請求項１２】
前記鍵が、対称鍵を含み、所定の鍵の同一のコピーが、前記クライアント上の安全なストレージ、及びサーバと関連付けられた安全なストレージ内に記憶される、請求項１１に記載のシステム。

【請求項１３】
前記鍵が、非対称鍵対を含み、前記鍵対の第１の鍵が、前記クライアント上の安全なストレージ内に記憶され、前記鍵対の第２の鍵が、サーバと関連付けられた安全なストレージ内に記憶される、請求項１１に記載のシステム。
【請求項１４】
前記鍵が、鍵プロビジョニングプロトコルを使用して送信される、請求項１１に記載のシステム。
【請求項１５】
前記鍵プロビジョニングプロトコルが、動的対称鍵プロビジョニングプロトコル（ＤＳＫＰＰ）を含む、請求項１４記載のシステム。
【請求項１６】
ユーザを認証するために前記認証デバイスのうちの少なくとも１つ及びその関連付けられた暗号エンティティを使用する手順が、
前記認証デバイスから生体ユーザ入力を受信する手順と、
前記生体ユーザ入力が前記ユーザの認証に成功したことを決定する手順と、
前記認証デバイスと関連付けられた前記暗号エンティティを使用して、サーバに送信される情報を暗号化する手順と、を含む、請求項１０に記載のシステム。
【請求項１７】
前記Ｎ個の認証デバイスが、生体認証デバイスを含み、
前記処理によって、前記Ｎ個の暗号エンティティを前記Ｎ個の認証デバイス毎に一つずつ発生する前に、前記クライアント上の前記Ｎ個の認証デバイスで前記ユーザをエンロールする手順が実行されることをさらに含む請求項１０に記載のシステム。
【請求項１８】
前記サーバが、特定の認証デバイスと関連付けられた暗号エンティティを使用して、前記クライアント及び／又は前記認証デバイスの身元を検証する、請求項１０に記載のシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、概して、データ処理システムの分野に関する。より具体的には、本発明は、認証能力を決定するためのクエリシステム及び方法に関する。
【背景技術】
【０００２】
既存のシステムは、生体センサを用いてネットワーク上で安全なユーザ認証を提供するために設計されている。具体的には、Ｆａｓｔ　Ｉｄｅｎｔｉｆｙ　Ｏｎｌｉｎｅ（ＦＩＤＯ）アライアンスによって開発されたＯｎｌｉｎｅ　Ｓｅｃｕｒｅ　Ｔｒａｎｓａｃｔｉｏｎ　Ｐｌｕｇｉｎ（ＯＳＴＰ）プロトコルは、強力な認証（例えば、個人情報の盗難及びフィッシング）、安全なトランザクション（例えば、トランザクションに対する「ブラウザ内のマルウェア」及び「中間者」攻撃）、並びにクライアント認証トークンのエンロールメント／管理（例えば、指紋読み取り器、顔認識デバイス、スマートカード、トラステッドプラットフォームモジュールなど）を可能にする。既存のＯＳＴＰプロトコルの詳細は、例えば、米国特許出願第２０１１／００８２８０１号（「８０１出願」）、及び表題「ＯＳＴＰ　Ｆｒａｍｅｗｏｒｋ」の文書（２０１１年3月２３日）で見つけることができ、これら両方ともにネットワーク上のユーザ登録及び認証のフレームワークについて説明する。
本発明のより良い理解は、以下の図面と併せて以下の詳細な説明から得ることができる。
【図面の簡単な説明】
【０００３】
【図１Ａ】安全な認証システムアーキテクチャの２つの異なる実施形態を図解する。

【図１Ｂ】安全な認証システムアーキテクチャの２つの異なる実施形態を図解する。
【図２】クライアントデバイス上の認証デバイスがどのように発見され得るかを示すトランザクション図である。
【図３】ユーザがどのように認証デバイスでエンロールし得るかを示すトランザクション図である。
【図４】鍵がどのように認証デバイスに登録され得るかを示すトランザクション図である。
【図５】ユーザ認証がどのように認証フレームワーク内で実装され得るかを示すトランザクション図である。
【図６】トランザクションの詳細がどのように検証され得るかを示すトランザクション図である。
【図７】本発明の一実施形態に従って実装されたクエリポリシーフィルタを図解する。
【図８】クエリポリシーとの登録動作がどのように本発明の一実施形態で実装されるかを示すトランザクション図である。
【図９】多重認証デバイス処理を実装するためのアーキテクチャの一実施形態を図解する。
【図１０Ａ】多重認証デバイス処理のための本発明の３つの実施形態を図解する。
【図１０Ｂ】多重認証デバイス処理のための本発明の３つの実施形態を図解する。
【図１０Ｃ】多重認証デバイス処理のための本発明の３つの実施形態を図解する。
【図１１Ａ】ランダムチャレンジのタイムアウトを検出し、それに応答するためのトランザクション図を図解する。
【図１１Ｂ】ランダムチャレンジのタイムアウトを検出し、それに応答するためのトランザクション図を図解する。
【図１２】本発明の一実施形態に従う、プライバシークラスを実装するためのアーキテクチャを図解する。
【図１３】本発明の一実施形態に従う、プライバシークラスを実装するためのトランザクション図である。
【図１４】認証するシグネチャ及びトランザクションを使用するためのアーキテクチャの一実施形態を図解する。
【図１５】本発明の実施形態を実行するためのコンピュータシステムの例示的な実施形態を図解する。
【図１６】本発明の実施形態を実行するためのコンピュータシステムの例示的な実施形態を図解する。
【発明を実施するための形態】
【０００４】
クライアントサーバ環境で認証フレームワークをインテリジェントに実装するための装置、方法、及び機械可読媒体の実施形態が以下に記載される。この説明全体を通して、説明のために、本発明の十分な理解を提供するために数多くの特定の詳細が記載される。しかしながら、本発明は、これらの特定の詳細のうちのいくつかを用いることなく実践され得ることが当業者に明らかであろう。他の例では、周知の構造及びデバイスは、示されないか、又は本発明の基本原理を不明瞭にすることを避けるために、ブロック図の形態で示される。
【０００５】
以下で論じられる本発明の実施形態は、生体デバイス等の認証能力を有するクライアントデバイスを含む。これらのデバイスは、本明細書において「トークン」と称され得る。指紋センサ、音声認識ハードウェア／ソフトウェア（例えば、マイクロホン、及びユーザの声を認識するための関連したソフトウェア）、顔認識ハードウェア／ソフトウェア（例えば、カメラ、及びユーザの顔を認識するための関連したソフトウェア）、光学的認識能力（例えば、光スキャナ、及びユーザの網膜を走査するための関連したソフトウェア）を含むが、これらに限定されない、様々な異なる生体デバイスが使用され得る。認証能力は

また、トラステッドプラットフォームモジュール（ＴＰＭ）及びスマートカード等の非生体デバイスを含むことができる。

【０００６】

以下に記載される本発明の実施形態は、既存の認証技術を上回る様々な改善を提供する。例えば、ネットワーク上でその認証能力の全て（例えば、その認証トークン／デバイスの全て）の包括的なリストを通信することをクライアントに要求する現在の技術とは対照的に、本発明の一実施形態は、安全なトランザクションサーバが最初に、サーバによって許容された認証能力を示すクライアントにサーバポリシーを送信するクエリポリシーを実装する。クライアントは次に、サーバポリシーを分析して、認証能力のサブセットを識別し、それによりクライアントへのプライバシーインパクトを減少させる。

【０００７】

別の実施形態では、複数の構成可能なプライバシー保護のレベルが利用される。プライバシークラスは事前に定義され、エンドユーザによって選択及び／又は修正され得る。本発明の一実施形態では、プライバシークラスは、クライアントが要求された情報を用いて識別され得る確率に基づいて定義される。比較的より高いプライバシーレベル（比較的より低いプライバシーインパクトを有する）では、クライアントデバイスに関する比較的より少ない情報は、本明細書に記載される認証技術を実施するために公表される。

【０００８】

本発明の別の実施形態は、同時に複数のデバイスのプロビジョニング又は認証を提供し、それにより効率を改善する。例えば、一度に単一の認証デバイスに対する登録又は認証を要求する代わりに、認証デバイスのリストがサーバから送信され得る。対称鍵及び／又は非対称鍵は次に、１つの動作、又はクライアント上でローカルに実行された一連の連続的動作で複数のトークン／デバイスにプロビジョニングされる。認証のために、いくつかのトークン／デバイスが所定のトランザクションに同時に選択され得る。

【０００９】

本発明の別の実施形態は、サーバのチャレンジが処理及び管理される効率を改善する。今日、サーバがランダムチャレンジをクライアントに送信した後（例えば、暗号ノンス）、クライアントが特定のタイムアウト期間内に応答しない場合、このノンスは、もはや有効ではなく、クライアントは、後続の認証の試みに応答してエラーを受信する。例えば、ユーザがクライアントを一時停止して、新しい位置に移動し（例えば、ラップトップ上の蓋を閉め）、次いで認証を試みる場合、認証の試みは拒否される。本発明の一実施形態では、クライアントは、ランダムチャレンジの期限が切れたことを検出し、サーバからの新しいチャレンジを自動的かつ透過的に要求する。サーバは次に、新しいチャレンジを生成し、それを、それが認証に使用され得るクライアントに送信するエンドユーザ経験は、ユーザが認証要求のエラー又は拒否を受信しないことにより改善される。

【００１０】

本発明の別の実施形態は、トランザクション状態がクライアントとの現在のセッションを維持するためにサーバ上に維持される必要がないように、安全なトランザクションサーバ上のトランザクション署名を利用する。トランザクションテキスト等のトランザクションコンテンツは、サーバによって署名されたクライアントに送信され、サーバが応答すると、それは、シグネチャと共にトランザクションコンテンツを送り返す。サーバは、クライアントによって受信された、署名されたトランザクション応答がシグネチャを検証することによって有効であることを検証することができることにより、トランザクション状態を記憶する必要がない。

【００１１】

別個の実施形態として上記に記載されるが、上記の技術の全ては、単一の包括的な認証システム内に様々な方法で共に組み合わせられ得る。したがって、本発明の所定の実施形態は、安全なネットワーク環境でクライアント及びユーザ認証を改善するために、本明細書に記載される１つ以上の他の実施形態と組み合わせられ得る。

【００１２】

例示的なシステムアーキテクチャ

図１Ａ～Ｂは、ユーザを認証するためのクライアント側及びサーバ側の構成要素を備えるシステムアーキテクチャの２つの実施形態を図解する。図１Ａに示される実施形態は、ウェブサイトと通信するためにブラウザプラグインベースのアーキテクチャを使用するが、図１Ｂに示される実施形態は、ブラウザを必要としない。認証デバイスでユーザをエンロールすること、安全なサーバで認証デバイスを登録すること、及びユーザを認証することなど、本明細書に記載される様々な技術は、これらのシステムアーキテクチャのいずれかに実装され得る。したがって、図１Ａに示されるアーキテクチャは、以下に記載される実施形態のうちのいくつかの動作を実証するために使用されるが、同一の基本原理は、図１Ｂに示されるシステム上で（例えば、サーバ１３０とクライアント上の安全なトランザクションサービス１０１との間の通信のための仲介としてブラウザプラグイン１０５を削除することによって）容易に実装され得る。

【００１３】

最初に図１Ａを参照すると、図解される実施形態は、エンドユーザをエンロール及び認証するために１つ以上の認証デバイス１１０～１１２（当該技術分野において、認証「トークン」と称される場合もある）が備えられたクライアント１００を含む。上記のように、認証デバイス１１０～１１２は、指紋センサ、音声認識ハードウェア／ソフトウェア（例えば、マイクロホン、及びユーザの声を認識するための関連したソフトウェア）、顔認識ハードウェア／ソフトウェア（例えば、カメラ、及びユーザの顔を認識するための関連したソフトウェア）、及び光学的認識能力（例えば、光スキャナ、及びユーザの網膜を走査するための関連したソフトウェア）等の生体デバイス、並びにトラステッドプラットフォームモジュール（ＴＰＭ）及びスマートカード等の非生体デバイスを含むことができる。

【００１４】

認証デバイス１１０～１１２は、安全なトランザクションサービス１０１によって明らかにされたインターフェース１０２（例えば、アプリケーションプログラミングインターフェース又はＡＰＩ）を通じてクライアントに通信可能に連結される。安全なトランザクションサービス１０１は、ネットワーク上で１つ以上の安全なトランザクションサーバ１３２～１３３と通信し、かつウェブブラウザ１０４の文脈において実行された安全なトランザクションプラグイン１０５と対話するための安全なアプリケーションである。図解されるように、インターフェース１０２はまた、デバイス識別コード、ユーザ識別コード、ユーザエンロールメントデータ（例えば、走査された指紋又は他の生体データ）、及び本明細書に記載される安全な認証技術を実施するために使用される鍵など、認証デバイス１１０～１１２の各々に関連する情報を記憶するクライアント１００上の安全なストレージデバイス１２０に安全なアクセスを提供することができる。例えば、以下で詳細に論じられるように、一意の鍵は、認証デバイスの各々に記憶され、インターネット等のネットワーク上でサーバ１３０に通信するときに使用され得る。

【００１５】

以下で論じられるように、ある特定のタイプのネットワークトランザクションは、ウェブサイト１３１又は他のサーバとのＨＴＴＰ又はＨＴＴＰＳトランザクションなど、安全なトランザクションプラグイン１０５によって支持される。一実施形態では、安全なトランザクションプラグインは、安全なエンタープライズ又はウェブ宛先１３０（以下で単に「サーバ１３０」と称される場合もある）内のウェブサーバ１３１によってウェブページのＨＴＭＬコードに挿入された特定のＨＴＭＬタグに応答して開始される。このようなタグを検出することに応答して、安全なトランザクションプラグイン１０５は、処理するために安全なトランザクションサービス１０１にトランザクションを転送することができる。加えて、ある特定のタイプのトランザクション（例えば、安全な鍵交換など）では、安全なトランザクションサービス１０１は、オンプレミスのトランザクションサーバ１３２（即ち、ウェブサイトと共同設置される）、又はオフプレミスのトランザクションサーバ１３３で直接的通信チャネルを開くことができる。

【００１６】
安全なトランザクションサーバ１３２～１３３は、ユーザデータ、認証デバイスデータ、鍵、及び以下に記載される安全な認証トランザクションを支持するために必要とされる他の安全な情報を記憶するために安全なトランザクションデータベース１２０に連結される。しかしながら、本発明の基本原理は、図１Ａに示される安全なエンタープライズ又はウェブ宛先１３０内の論理構成要素の分離を必要としないことに留意されたい。例えば、ウェブサイト１３１及び安全なトランザクションサーバ１３２～１３３は、単一の物理サーバ又は別個の物理サーバ内に実装され得る。更に、ウェブサイト１３１及びトランザクションサーバ１３２～１３３は、以下に記載される機能を果たすために１つ以上のサーバ上で実行される統合ソフトウェアモジュール内に実装され得る。
【００１７】
上記のように、本発明の基本原理は、図１Ａに示されるブラウザベースのアーキテクチャに限定されない。図１Ｂは、スタンドアロン型アプリケーション１５４が安全なトランザクションサービス１０１によって提供された機能を利用して、ネットワーク上でユーザを認証する代替の実装形態を図解する。一実施形態では、アプリケーション１５４は、以下に詳細に記載されるユーザ／クライアント認証技術を実施するために安全なトランザクションサーバ１３２～１３３に依存する１つ以上のネットワークサービス１５１と通信セッションを確立するように設計される。
【００１８】
図１Ａ～Ｂに示される実施形態のいずれかでは、安全なトランザクションサーバ１３２～１３３は、次に安全なトランザクションサービス１０１に安全に送信され、かつ安全なストレージ１２０内の認証デバイスに記憶される鍵を生成することができる。加えて、安全なトランザクションサーバ１３２～１３３は、サーバ側で安全なトランザクションデータベース１２０を管理する。
【００１９】
デバイス発見、エンロールメント、登録、及び認証の概要
認証デバイス発見、エンロールメント、登録、及び認証を実施するための例示的な一連のトランザクションが図２～６に示される。これらのトランザクションのいくつかの態様は、上述されるＯＳＴＰプロトコルで利用されている（更なる詳細は、ＯＳＴＰ　Ｆｒａｍｅｗｏｒｋ（２０１１年3月２３日）を参照され、これは、参照により本明細書に組み込まれる）。これらのトランザクションの基本動作の理解は、本発明の実施形態が実装され得る状況を提供する。
【００２０】
以下に記載される動作は、認証デバイスの検出（図２）、認証デバイスでのユーザのエンロールメント（図３）、認証デバイスの登録（図４）、登録された認証デバイスでのユーザ認証（図５）、及び認証後の安全なトランザクションの実装（図６）を含む。
【００２１】
図２は、クライアントマシン上で認証デバイスを検出するための一連のトランザクションを図解する。デバイス検出の完了に成功した後、サーバ１３０は、クライアントに取り付けられた認証デバイスに関する包括的な情報を保有し、どのデバイス（複数可）が強化されたセキュリティ基盤と共に使用するのに最も適切であるかを評価することができる。サーバ１３０のみ、認証デバイスのリストをフィルタリングする。ユーザには、このリストが提供され、ユーザは、認証デバイスのうちの１つ（又は組み合わせ）を選択して、安全なトランザクションの更なる認証及び実装のために使用することができる。
【００２２】
動作中、ユーザは、ブラウザ内のユーザ名及びパスワードで認証し、ウェブサイトにログインする。これは、ユーザがユーザ名及びパスワードを提供することを求められる唯一の時間である。サーバ１３０は、ユーザが強化されたセキュリティを現在使用していないことを（例えば、安全なトランザクションデータベース１２０に問い合わせることによって）決定し、強化されたセキュリティに変更する提案をユーザに提供する。

【００２３】
一実施形態では、サーバ１３０は、安全なトランザクションプラグイン１０５が検出するＨＴＭＬページ内の「デバイスに関するクエリ」タグを含む。タグを検出することに応答して、安全なトランザクションプラグイン１０５は、この要求を安全なトランザクションサービス１０１に再経路指定し、これは次に、デバイスのセキュリティ特性を含むシステムに取り付けられた全ての認証デバイスに関する包括的な情報を用意する。一実施形態では、この情報は、事前に指定されたデータスキーマを用いて送信より前にＸＭＬフォーマットでパッケージ化される。
【００２４】
安全なトランザクションプラグイン１０５は、安全なトランザクションサービス１０１からこの情報を受信し、一実施形態では、登録されたコールバックによってウェブページのＪａｖａＳｃｒｉｐｔ（登録商標）にこの情報を渡す。これは次に、この情報をブラウザ１０４にどのように表示するかを選択する。ウェブサイトによってフィルタリングされたリストは、ユーザに示されてもよく、ユーザは、認証デバイスのうちの１つ又は組み合わせを選択してもよい。
【００２５】
図３は、認証デバイスでユーザをエンロールする一連のトランザクションを図解する。一実施形態では、エンロールメントは、本明細書に記載される本発明の実施形態によって提供される強化されたセキュリティを使用するための必要条件である。エンロールメントは、後続のトランザクションの間、同一の認証デバイスがユーザを認証するために使用され得るように、ユーザの生体読み取り（例えば、指紋、音声サンプルなど）を記録することを含む。エンロールメント動作は、サーバ１３０との対話を用いることなく、単にクライアント上で行われ得る。エンロールメントのために提供されたユーザインターフェース（複数可）は、ブラウザ拡張で表示されてもよく、又は別個のアプリケーション若しくはモバイルデバイスのアプリに表示されてもよい。
【００２６】
エンロールメント動作は、デバイスが検出されるとすぐに開始され得る。ユーザは、強化されたセキュリティに対して発見されたデバイスのうちの１つ又はその一群を使用するために選択することができる。動作中、ユーザは、ブラウザ内の表示されたデバイスリスト、アプリケーション、又はモバイルデバイスのアプリからデバイスを選択することができる。図３に図解されるブラウザベースの実装形態では、安全なトランザクションプラグイン１０５は、デバイス固有のエンロールメントのグラフィカルユーザインターフェース（ＧＵＩ）を表示する。安全なトランザクションプラグイン１０５は、デバイス識別子及びエンロールメント要求を安全なトランザクションサービス１０１に送信し、完了を待つ。ユーザが既にクライアント上の認証デバイスでエンロールされた場合、ユーザは単に、それらの身元を検証する必要があり得る（即ち、それらは、再度エンロールすることを必要とされない）。ユーザが現在エンロールされていない場合、安全なトランザクションサービス１０１は、物理的な認証デバイスを起動することによって（例えば、デバイスインターフェース１０２を介して）エンロールメントプロセスを開始する。ユーザは次に、安全なトランザクションプラグイン１０５のＧＵＩと対話し、指定されたエンロールメントステップ（例えば、指をスワイプすること、マイクロホンに向かって話すこと、スナップ写真を撮ること）に従う。完了すると、ユーザは、認証デバイスでエンロールされる。意義深いことに、ユーザがデバイスでエンロールされると、それらは、このエンロールメントを使用して、本明細書に記載されるような任意のウェブサイト又はネットワークサービスで登録又は認証することができる。
【００２７】
図４は、認証デバイスの登録のための一連のトランザクションを図解する。登録中、鍵は、認証デバイスと安全なトランザクションサーバ１３２～１３３のうちの１つとの間で共有される。鍵は、クライアント１００の安全なストレージ１２０、及び安全なトランザクションサーバ１３２～１３３によって使用される安全なトランザクションデータベース

１２０内に記憶される。一実施形態では、鍵は、安全なトランザクションサーバ１３２～１３３のうちの１つによって生成された対称鍵である。しかしながら、以下で論じられる別の実施形態では、非対称鍵が使用され得る。この実施形態では、公開鍵は、安全なトランザクションサーバ１３２～１３３によって記憶され得、第２の関連した秘密鍵は、クライアント上の安全なストレージ１２０内に記憶され得る。更に、一実施形態（以下にも論じられる）では、鍵（複数可）は、クライアント１００上で（例えば、安全なトランザクションサーバ１３２～１３３ではなく、認証デバイス又は認証デバイスのインターフェースによって）生成され得る。

【００２８】

動的対称鍵プロビジョニングプロトコル（ＤＳＫＰＰ）等の安全な鍵プロビジョニングプロトコルは、安全な通信チャネル上でクライアントと鍵を共有するために使用され得る（例えば、Ｒｅｑｕｅｓｔ　ｆｏｒ　Ｃｏｍｍｅｎｔｓ（ＲＦＣ）６０６３参照）。しかしながら、本発明の基本原理は、任意の特定の鍵プロビジョニングプロトコルに限定されない。

【００２９】

図４に示される特定の詳細を参照すると、ユーザエンロールメント又はユーザ認証が完了すると、サーバ１３０は、デバイス登録中にクライアントによって提示されなければならないランダムに生成されたチャレンジ（例えば、暗号ノンス）を生成する。ランダムチャレンジは、限定された期間有効であり得る。安全なトランザクションプラグインは、ランダムチャレンジを検出し、それを安全なトランザクションサービス１０１に転送する。それに応答して、安全なトランザクションサービスは、サーバ１３０と帯域外セッション（例えば、帯域外トランザクション）を開始し、鍵プロビジョニングプロトコルを用いてサーバ１３０と通信する。サーバ１３０は、ユーザ名でユーザを特定し、ランダムチャレンジの有効性を確認し、送信された場合にデバイスの認証コードの有効性を確認し、ユーザに対して安全なトランザクションデータベース１２０内に新しいエントリを作成する。これはまた、鍵を生成し、鍵をデータベース１２０に書き込み、鍵プロビジョニングプロトコルを用いて安全なトランザクションサービス１０１に鍵を送り返すことができる。完了すると、認証デバイス及びサーバ１３０は、対称鍵が使用された場合に同一の鍵を、又は非対称鍵が使用された場合に異なる鍵を共有する。

【００３０】

図５は、登録された認証デバイスでのユーザ認証のための一連のトランザクションを図解する。デバイス登録が完了すると、サーバ１３０は、有効な認証トークンとしてローカル認証デバイスによって生成されたトークンを受け取る。

【００３１】

ブラウザベースの実装形態を示す、図５に示される特定の詳細を参照すると、ユーザは、ブラウザ１０４内にサーバ１３０のユニフォームリソースロケータ（ＵＲＬ）を入力する。スタンドアロン型アプリケーション又はモバイルデバイスのアプリ（ブラウザではなく）を使用する実装形態では、ユーザは、ネットワークサービスのネットワークアドレスを入力することができ、又はアプリケーション若しくはアプリは、ネットワークアドレスでネットワークサービスに接続することを自動的に試みることができる。

【００３２】

ブラウザベースの実装形態では、ウェブサイトは、ＨＴＭＬページ内に登録されたデバイスに関するクエリを埋め込む。これは、Ｊａｖａｓｃｒｉｐｔ（登録商標）によって、又はＨＴＴＰヘッダなどを用いて、ＨＴＭＬページ内にクエリを埋め込む以外に多くの方法で行われ得る。安全なトランザクションプラグイン１０５は、ＵＲＬを受信し、それを安全なトランザクションサービス１０１に送信し、これは、安全なストレージ１２０（論じられるように、認証デバイス及びユーザ情報のデータベースを含む）を検索し、それを調査し、このＵＲＬ内にエンロールされたユーザがいるかを決定する。いるのであれば、安全なトランザクションサービス１０１は、このＵＲＬ関連付けられたプロビジョニングされたデバイスのリストを安全なトランザクションプラグイン１０５に送信する。安全な

トランザクションプラグインは次に、登録されたＪａｖａＳｃｒｉｐｔ（登録商標）のＡＰＩを呼び出し、この情報をサーバ１３０（例えば、ウェブサイト）に渡す。サーバ１３０は、送信されたデバイスリストから適切なデバイスを選択し、ランダムチャレンジを生成し、デバイス情報を送信し、引数をクライアントに送り返す。ウェブサイトは、対応するユーザインターフェースを表示し、ユーザから認証を要求する。ユーザは次に、要求された認証評価基準（例えば、指紋読取器にわたって指をスワイプすること、音声認識のために話すことなど）を提供する。安全なトランザクションサービス１０１は、ユーザを識別し（このステップは、ユーザを記憶することを支持しないデバイスに対して飛ばして進むことができる）、データベースからユーザ名を取得し、鍵を使用して認証トークンを生成し、安全なトランザクションプラグインを介してこの情報をウェブサイトに送信する。サーバ１３０は、安全なトランザクションデータベース１２０からユーザを識別し、サーバ１３０上に同一のトークンを生成することによって（例えば、鍵のコピーを用いて）トークンを検証する。検証されると、認証プロセスは完了する。

【００３３】

図６は、ブラウザベースの実装形態のための認証後の安全なトランザクションを図解する。安全なトランザクションは、ある特定のタイプのトランザクション（例えば、金融取引）に対するより強力なセキュリティを提供するように設計される。図解される実施形態では、ユーザは、トランザクションを完遂するより前に各トランザクションを確認する。図解される技術を用いて、ユーザは、ユーザが完遂することを望むものを正確に確認し、ユーザがＧＵＩ内に表示された見るものを正確に完遂する。換言すれば、本実施形態は、ユーザが確認しなかったトランザクションを完遂するために、トランザクションテキストが「中間者」によって修正され得ないことを確実にする。

【００３４】

一実施形態では、安全なトランザクションプラグイン１０５は、トランザクション詳細を示すブラウザ関連でウィンドウ６０１を表示する。安全なトランザクションサーバ１０１は定期的に（例えば、ランダムな間隔で）、ウィンドウに示されるテキストが誰にも改ざんされていないかを検証する。

【００３５】

以下の例は、本実施形態の動作を強調するのに役立つであろう。ユーザは、商人のサイトから購入のための品目を選択し、「チェックアウト」を選択する。商人のサイトは、本明細書に記載される本発明の実施形態のうちの１つ以上を実装する安全なトランザクションサーバ１３２～１３３を有するサービスプロバイド（例えば、ＰａｙＰａｌ）にトランザクションを送信する。商人のサイトは、ユーザを認証し、トランザクションを完了する。

【００３６】

安全なトランザクションサーバ１３２～１３３は、トランザクション詳細（ＴＤ）を受信し、「Ｓｅｃｕｒｅ　Ｔｒａｎｓａｃｔｉｏｎ」要求をＨＴＭＬページ内に入れ、クライアント１００に送信する。Ｓｅｃｕｒｅ　Ｔｒａｎｓａｃｔｉｏｎ要求は、トランザクション詳細及びランダムチャレンジ（例えば、ランダムノンス）を含む。安全なトランザクションプラグイン１０５は、トランザクション確認メッセージに対する要求を検出し、全てのデータを安全なトランザクションサービス１０１に転送する。ブラウザ又はプラグインを使用しない実施形態では、情報は、安全なトランザクションサーバからクライアント１００上の安全なトランザクションサービスに直接送信され得る。

【００３７】

ブラウザベースの実装形態では、安全なトランザクションプラグイン１０５は、ユーザへのトランザクション詳細（ブラウザ関連における）でウィンドウ６０１を表示し、トランザクションを確認する認証を提供することをユーザに求める。ブラウザ又はプラグインを使用しない実施形態では、安全なトランザクションサービス１０１又はアプリケーション１５４は、ウィンドウ６０１を表示することができる。安全なトランザクションサービス１０１は、タイマーを開始し、ユーザに表示されているウィンドウ６０１の内容を検証

する。検証の期間は、ランダムに選択され得る。安全なトランザクションサービス１０１は、ユーザがウィンドウ６０１内の有効なトランザクション詳細を見ることを確実にする。コンテンツが改ざんされたことを検出する場合、これは、確認トークンが生成されることを防ぐ。

【００３８】

ユーザが有効な認証を提供した（例えば、指紋センサ上で指をスワイプした）後、デバイスは、ユーザを識別し、トランザクション詳細及びランダムチャレンジでトークン（暗号シグネチャ）を生成する（即ち、トークンは、トランザクション詳細及びノンス上で計算される）。これにより、安全なトランザクションサーバ１３２～１３３はトランザクション詳細がサーバとクライアントとの間で修正されていないことを確実にすることができる。安全なトランザクションサービス１０１は、生成されたトークン及びユーザ名を安全なトランザクションプラグイン１０５に送信し、これは、トークンを安全なトランザクションサーバ１３２～１３３に転送する。安全なトランザクションサーバ１３２～１３３は、ユーザ名でユーザを識別し、トークンを検証する。検証が成功した場合、確認メッセージがクライアントに送信され、トランザクションが処理される。

【００３９】

クライアント認証能力を決定する安全なクエリポリシーのためのシステム及び方法

述べられるように、本発明の一実施形態は、安全なトランザクションサーバがサーバによって許容される認証能力を示すサーバポリシーをクライアントに送信するクエリポリシーを実装する。クライアントは次に、サーバポリシーを分析して、それが支持し、及び／又はユーザが使用する要求を示した認証能力のサブセットを識別する。クライアントは次に、提供されたポリシーと一致する認証トークンのサブセットを用いてユーザを登録及び／又は認証する。その結果として、クライアントがその認証能力（例えば、その認証デバイスの全て）に関する包括的な情報、又はクライアントを一意的に識別するために使用され得る他の情報を送信することを必要とされないため、クライアントのプライバシーへのインパクトの低下がある。

【００４０】

例として、限定ではなく、クライアントは、２～３例を挙げると、指紋センサ、音声認識能力、顔認識能力、目／光学的認識、トラステッドプラットフォームモジュール（ＴＰＭ）、及びスマートカードなどの数多くの認証能力を含むことができる。しかしながら、プライバシーの理由で、ユーザは、その能力の全てに対する詳細を要求するサーバに公表することを望まない場合がある。したがって、本明細書に記載される技術を用いると、安全なトランザクションサーバは、それが、例えば、指紋、光、又はスマートカード認証を支持することを示すサーバポリシーをクライアントに送信することができる。クライアントは次に、サーバポリシーと独自の認証能力とを比較し、利用可能な認証オプションのうちの１つ以上を選択することができる。

【００４１】

図７は、これらの技術を実装するためのクライアントサーバアーキテクチャの一実施形態を図解する。図解されるように、クライアント１００上に実装された安全なトランザクションサービス１０１は、サーバ１３０によって提供されたポリシーを分析し、かつ登録及び／又は認証に使用される認証能力のサブセットを識別するためのポリシーフィルタ７０１を含む。一実施形態では、ポリシーフィルタ７０１は、安全なトランザクションサービス１０１の文脈において実行されたソフトウェアモジュールとして実装される。しかしながら、ポリシーフィルタ７０１は、本発明の基本原理に依然として適合しながら任意の様式で実装されてもよく、ソフトウェア、ハードウェア、ファームウェア、又はこれらの任意の組み合わせを含んでもよいことに留意されたい。

【００４２】

図７に示される特定の実装形態は、前述の技術を用いて安全なエンタープライズ又はウェブ宛先１３０（単に「サーバ１３０」と称される場合もある」）との通信を確立するための安全なトランザクションプラグイン１０５を含む。例えば、安全なトランザクション

プラグインは、ウェブサーバ１３１によってＨＴＭＬコードに挿入された特定のＨＴＭＬタグを識別することができる。したがって、この実施形態では、サーバポリシーは、ポリシーフィルタ７０１を実装する安全なトランザクションサービス１０１にそれを転送する安全なトランザクションプラグイン１０５に提供される。

【００４３】

ポリシーフィルタ７０１は、クライアントの安全なストレージ領域７２０から能力を読み取ることによってクライアント認証能力を決定することができる。前述のように、安全なストレージ７２０は、クライアントの認証能力（例えば、認証デバイスの全てに対する識別コード）の全てのリポジトリを備えることができる。ユーザがその認証デバイスでユーザを既にエンロールしている場合、ユーザのエンロールメントデータは、安全なストレージ７２０内に記憶される。クライアントがサーバ１３０で認証デバイスを既に登録している場合、安全なストレージはまた、各認証デバイスと関連付けられた暗号化された秘密鍵を記憶することができる。

【００４４】

安全なストレージ７２０から抽出された認証データ、及びサーバによって提供されたポリシーを用いて、ポリシーフィルタ７０１は次に、使用される認証能力のサブセットを識別することができる。構成に応じて、ポリシーフィルタ７０１は、クライアント及びサーバの両方によって支持された認証能力の全リストを識別することができ、又は全リストのサブセットを識別することができる。例えば、サーバが認証能力Ａ、Ｂ、Ｃ、Ｄ、及びＥを支持し、クライアントが認証能力Ａ、Ｂ、Ｃ、Ｆ、及びＧを有する場合、ポリシーフィルタ７０１は、サーバＡ、Ｂ、及びＣに対する共通の認証能力のサブセット全体を識別することができる。あるいは、図７におけるユーザ選好７３０によって示されるように、より高いプライバシーレベルが所望される場合、より限定された認証能力のサブセットがサーバに識別され得る。例えば、ユーザは、単一の共通認証能力のみがサーバ（例えば、Ａ、Ｂ、又はＣのうちの１つ）に識別されるべきであることを示すことができる。一実施形態では、ユーザは、クライアント１００の認証能力の全てに対して優先順位付け計画を確立することができ、ポリシーフィルタは、サーバ及びクライアントの両方に共通の最高優先認証能力（又は優先順位付けされたＮ個の認証能力のセット）を選択することができる。

【００４５】

どの動作がサーバ１３０によって開始されているか（登録又は認証）に応じて、安全なトランザクションサービス１３０は、フィルタリングされた認証デバイス（１１０～１１２）のサブセット上でその動作を実施し、図７に示されるように、安全なトランザクションプラグイン１０５を介してサーバ１３０に動作応答を送り返す。あるいは、ウェブブラウザのプラグイン１０５構成要素に依存しない実施形態では、情報は、安全なトランザクションサービス１０１からサーバ１３０に直接渡され得る。

【００４６】

図８は、クエリポリシートランザクションによる例示的な一連の登録のための更なる詳細を示すトランザクション図を図解する。図解される実施形態では、ユーザは、サーバ１３０でデバイスを以前に登録していない。その結果として、８０１では、ユーザは、初期の一時的認証ステップとしてユーザ名及びパスワードを入力することができ、これは８０２で、クライアントブラウザ１０４を介してサーバ１３０に転送される。しかしながら、ユーザ名及びパスワードは、本発明の基本原理に適合するために必要とされないことに留意されたい。

【００４７】

ユーザが８０３で決定された強化されたセキュリティで以前に登録していなかったため、サーバ１３０は、８０４でそのサーバポリシーをクライアントに送信する。述べられるように、サーバポリシーは、サーバ１３０によって支持された認証能力の表示を含むことができる。図解される例では、サーバポリシーはトランザクション８０６を介して安全なトランザクションサービス１０１に渡される。

【００４８】
トランザクション８０７では、安全なトランザクションサービス１０１は、サーバポリシーをクライアントの能力（及び潜在的に、上記に記載されるようなデバイス優先計画及び／又はユーザ選好などの他の情報）と比較して、フィルタリングされた認証能力のリストを導出する。フィルタリングされたデバイス（１０２）のリストは次に、鍵を生成し（８０８及び８０９）、次いでこれらの鍵の公開部分を安全なトランザクションサービス１０１に提供し、これはその順に、登録応答としてこれらをサーバ１３０に送り返す。サーバは、認証デバイスを証明し、安全なトランザクションデータベース内に公開鍵を記憶する。本明細書に利用されるトークン証明は、登録中の認証デバイスの身元の有効性を確認するプロセスである。これにより、サーバはクライアントによって報告されたデバイスが真に主張されるものであることを暗号で確認することができる。
【００４９】
あるいは又は加えて、８０７では、ユーザには、リストを再検討し、及び／又はこの特定のサーバ１３０と共に使用される特定の認証能力を選択する機会が提供され得る。例えば、フィルタリングされたリストは、指紋スキャン、顔認識、及び／又は音声認識による認証を使用するオプションを示すことができる。ユーザは次に、サーバ１３０で認証するとき、これらのオプションのうちの１つ以上を使用するために選択することができる。
【００５０】
クライアントでサーバポリシーをフィルタリングするための上記に記載される技術は、上記に記載される一連のトランザクションの様々な異なる段階（例えば、デバイス発見、デバイス登録、デバイスプロビジョニング、ユーザ認証中など）で実装され得る。即ち、本発明の基本原理は、図８に記載される特定のトランザクションのセット及び特定のトランザクション順序付けに限定されない。
【００５１】
更に、前述のように、ブラウザプラグインアーキテクチャは、本発明の基本原理に適合するために必要とされない。ブラウザ又はブラウザプラグイン（例えば、スタンドアロン型アプリケーション又はモバイルデバイスのアプリ）を含むアーキテクチャでは、図８に示されるトランザクション図（及び本明細書に開示される残りのトランザクション図）は、ブラウザ１０４が削除されるように単純化されてもよく、安全なトランザクションサービス１０１は、サーバ１３０と直接通信する。
【００５２】
複数の認証デバイスで効率的にエンロール、登録、及び認証するためのシステム及び方法
本発明の一実施形態は、同時に複数のデバイスをエンロール、登録、及び認証し、それにより効率及びユーザ経験を改善することができる。例えば、一度に単一デバイスに対する登録及び認証を要求する代わりに、デバイスのリストがクライアントに送信され得る。対称鍵又は非対称鍵は次に、１つの動作、又はクライアント上でローカルに実行された一連の連続的動作で複数のデバイスに登録され得る。認証のために、いくつかのトークン／デバイスが所定のトランザクションに同時に選択され得る。
【００５３】
図９は、これらの技術を実装するためのクライアントサーバアーキテクチャの一実施形態を図解する。図解されるように、クライアント１００上に実装された安全なトランザクションサービス１０１は、各デバイスがエンロール／登録されるとき、サーバ１３０との連続的な往復通信の必要なく、一度に複数のデバイスのエンロールメント及び登録などの指定された動作を実施するためのマルチデバイス処理論理９０１を含む。同様に、サーバ１３０は、複数の認証デバイスに方向付けられたコマンドを発行するためのマルチデバイス処理論理を含む。一実施形態では、マルチデバイス処理論理９０１は、安全なトランザクションサービス１０１の文脈において実行されたソフトウェアモジュールとして実装される。しかしながら、マルチデバイス処理論理９０１は、本発明の基本原理に依然として適合しながら任意の様式で実装されてもよく、ソフトウェア、ハードウェア、ファームウ

ェア構成要素、又はこれらの任意の組み合わせを含んでもよいことに留意されたい。

【００５４】

上記に記載される実施形態のように、図９に示される特定の実装形態は、サーバ１３０との通信を確立するための安全なトランザクションプラグイン１０５を含む（論じられるように、ウェブサイトサーバ１３１及び安全なトランザクションサーバ１３２～１３３を含むことができる）。したがって、サーバ１３０は、安全なトランザクションプラグイン１０５を介して安全なトランザクションサービス１０１と通信する。しかしながら、述べられるように、ブラウザベースのプラグインアーキテクチャは、本発明の基本原理に適合するために必要とされない。

【００５５】

サーバ１３０上のマルチデバイス処理論理９０２は、複数の認証デバイス１１０～１１２上でこれらの動作を実施するクライアント１００上のマルチデバイス処理論理９０１によって実行されるコマンドを通信することができる。例として、マルチデバイス処理論理９０２は、Ｎ個の認証デバイスの各々で登録されるＮ個の鍵を生成し、次いでＮ個のデバイスを登録するコマンドコマンドと共にマルチデバイス処理論理９０１に安全に送信することができる。マルチデバイス処理論理９０１は次に、サーバとの更なる対話を用いることなくＮ個のデバイス全てに（例えば、認証デバイス１１０～１１２に）、同時に又は一連の連続的動作で登録を実施することができる。次に、単一応答がサーバ１３０に送信されて、Ｎ個のデバイス全ての完了した登録を示すことができる。

【００５６】

一連の例示的なマルチデバイストランザクションが図１０Ａ～Ｃに図解される。図１０Ａは、サーバ１３０とのいずれの対話を用いることなく実施され得る（例えば、認証デバイスでユーザをエンロールすることがクライアント上の安全なトランザクションサービス１０１の制御下で実施され得る）マルチデバイスのエンロールメントプロセスを図解する。代替の実施形態では、サーバ１３０は、クライアント（図示せず）に対する要求を送信して、Ｎ個のデバイスでユーザをエンロールすることができる。図１０Ｂ～Ｃは、サーバ１３０で複数のデバイスを登録するための２つの異なる実施形態を図解する。

【００５７】

図１０Ａにおけるエンロールメントプロセスを参照すると、１００１では、ユーザは、クライアント上のＮ個の認証デバイスでエンロールする要求を示す（利用可能な認証デバイスの全て又はサブセットを表す）。それに応答して、安全なトランザクションプラグインは、１００２で呼び出され、１００３では、デバイス固有のグラフィカルユーザインターフェース（ＧＵＩ）は、プロセスを通じて、又は認証デバイス＃　１でエンロールすることによってユーザに付き添うように生成される。エンロールメントプロセスの間、ユーザは、示されるように（例えば、指紋センサ上に指を位置決めすること、マイクロホンに向かって話すこと、カメラでスナップ写真を撮ることなどによって）安全なトランザクションプラグインと対話する。一実施形態では、エンロールメントが１００４でＮ番目のデバイスに対して完了するまで、エンロールメントがＮ個のデバイスの各々に実施される。異なるデバイス固有のスクリプト及び／又はユーザインターフェースは、各個々の認証デバイスでユーザをエンロールするためにユーザに提示され得る。前述のように、ユーザが各デバイスでエンロールすると、ユーザエンロールメントデータは、クライアント１００上の安全なストレージ７２０内に記憶され、安全なトランザクションサービス１０１によってのみアクセス可能にされ得る。Ｎ個のデバイス全てに対するエンロールメントが完了すると、通知がトランザクション１００４～１００５を介してサーバ１３０に送信され得る。

【００５８】

エンロールメントがどのように実施されるかにかかわらず、完了すると、図１０Ｂに示されるトランザクション図は、サーバ１３０でＮ個のデバイスを登録するために使用され得る。１０１０では、サーバ１３０は、ユーザ固有のランダムチャレンジを生成し、これは、前述のように、制限された時間のウィンドウにのみ有効であり得、暗号ノンス等のラ

ンダムに生成されたコードを含み得る。１０１１では、ランダムチャレンジは、サーバ１３０でＮ個の認証デバイスを登録するコマンドと共に送信される。１０１２では、安全なトランザクションサービス１０１は、サーバ１３０と安全な接続を形成し、ランダムチャレンジと共にＮ個のデバイスに対する識別データを送信する。一実施形態では、安全な接続は、ＨＴＴＰＳ接続である。しかしながら、本発明の基本原理は、任意の特定の安全な接続タイプに限定されない。

【００５９】

１０１３では、サーバ１３０は、Ｎ個のデバイスを証明し、Ｎ個のデバイスの各々に鍵を生成し、安全な接続上でＮ個の鍵を安全なトランザクションサービスに送り返す。一実施形態では、動的対称鍵プロビジョニングプロトコル（ＤＳＫＰＰ）は、安全な接続上でクライアントと鍵を交換するために使用される。しかしながら、本発明の基本原理は、任意の特定の鍵プロビジョニング技術に限定されない。あるいは、ＤＳＫＰＰプロトコルに依存しない実施形態では、鍵は、各認証デバイスで生成され、次いでサーバ１３０に送信され得る。

【００６０】

１０１４～１０１５では、安全なトランザクションサービスのマルチデバイス処理論理は、Ｎ個の鍵の各々をＮ個のデバイスの各々に登録する。前述のように、各鍵は記憶され、クライアント上の安全なストレージ７２０内のそのそれぞれのデバイスと関連付けられ得る。各認証デバイスに対する登録が完了すると、１０１６で安全な接続上のサーバに通知が送信される。

【００６１】

一実施形態では、各認証デバイスに登録された鍵は、対称鍵である。したがって、各鍵の同一のコピーは、クライアント上の安全なストレージ７２０、及びサーバ１３０上の安全なトランザクションデータベース１２０内に記憶される。代替の実装形態では、非対称鍵対が生成され、この鍵のうちの１つがサーバ上の安全なトランザクションデータベース１２０内の公開鍵として維持され、秘密鍵は、クライアントの安全なストレージ７２０内に記憶される。しかしながら、本発明の基本原理は、任意の特定のタイプの暗号鍵に限定されないことに留意されたい。

【００６２】

代替の実装形態は、鍵がサーバ１３０ではなくクライアント上に生成される図１０Ｃに図解される。この実装形態では、１０１１においてランダムチャレンジでデバイスを登録する要求を受信した後、安全なトランザクションサービス１０１のマルチデバイス処理論理は、１１２０でＮ個のデバイスの各々に対するＮ個の鍵を生成する。生成されると、鍵は、１０１３～１０１４でＮ個のデバイスの各々で登録され、登録は、前述のように安全なストレージ７２０内に記憶される。全てのカギが登録されると、安全なトランザクションサービス１０１は、ランダムチャレンジと共に（クライアントの身元を検証するために）１０１５でサーバに通知を提供する。サーバ１３０は次に、上記に記載されるように安全なトランザクションデータベース１２０内に登録を記憶することができる。

【００６３】

認証フレームワーク内でランダムチャレンジを処理するためのシステム及び方法

本発明の一実施形態は、ランダムチャレンジがサーバによって生成され、かつ処理される有人型を改善する。一実施形態では、ランダムチャレンジは、暗号ノンス等のランダムに生成されたコードを含む。現在のシステムでは、サーバがクライアントにランダムチャレンジを送信した後、クライアントが特定のタイムアウト期間内に応答しない場合、ランダムチャレンジは、もはや有効ではなく、クライアントは、後続の認証の試みに応答してエラーを受信する（例えば、ユーザは、指紋読み取り器上で指をスワイプし、拒否される）。

【００６４】

本発明の一実施形態では、クライアントは、チャレンジの期限が切れ、サーバから新しいチャレンジを透過的に（即ち、ユーザが操作することなく）要求することを自動的に検

出する。サーバは次に、新しいランダムチャレンジを生成し、それをクライアントに送信し、これはその後、それを使用して、サーバとの安全な通信を確立する。エンドユーザ経験は、ユーザが認証要求のエラー又は拒否を受信しないことにより改善される。

【００６５】

図１１Ａは、登録プロセスの文脈において使用されるこのような１つの実施形態を図解し、図１１Ｂは、認証プロセスの文脈において使用される一実施形態を図解する。しかしながら、本発明の基本原理は、図１１Ａ～Ｂに示されるもの以外の状況で利用され得ることに留意されたい。例えば、本明細書に記載される技術は、時間依存コードがサーバからクライアントに通信される任意のプロセスと共に使用され得る。

【００６６】

最初に、図１１Ａを参照すると、１１０１では、サーバ１３０は、ランダムチャレンジ及びタイムアウト期間の表示を生成する。一実施形態では、タイムアウト期間は、ランダムチャレンジが有効と見なされる期間を含む。タイムアウト期間が経過した後、ランダムチャレンジは、サーバ１３０によってもはや有効と見なされない。一実施形態では、タイムアウト期間は、ランダムチャレンジがもはや有効ではない時点として単純に指定される。この時点に達すると、ランダムチャレンジは無効である。別の実施形態では、タイムアウト期間は、現在のタイムスタンプ（即ち、ランダムチャレンジがサーバ１３０によって生成される時間）及び継続時間を使用することによって指定される。安全なトランザクションサービス１０１は次に、ランダムチャレンジが無効になる時点を計算するために経過時間値をタイムスタンプに追加することによってタイムアウト期間を計算することができる。しかしながら、本発明の基本原理は、タイムアウト期間を計算するための任意の特定の技術に限定されないことに留意されたい。

【００６７】

タイムアウト期間がどのように指定又は計算されるかにかかわらず、１１０２では、ランダムチャレンジ及びタイムアウト表示は、安全なトランザクションサービス１０１に（図解される例ではブラウザ１０４及び安全なトランザクションプラグイン１０５を介して）送信される。１１０３では、安全なトランザクションサービス１０１は、ランダムチャレンジがタイムアウトし、サーバ１３０から送信されたタイムアウト表示に基づいてもはや有効ではないことを検出する。例として、ユーザは、一連のトランザクションを完了するより前にユーザのクライアントマシンの電源を切るか、又はユーザのノートブックコンピュータ上の蓋を閉じてもよい。トランザクションがユーザとの対話を必要とするものである場合、ユーザは、単純に立ち去るか、又はＧＵＩ内に表示されるメッセージを無視してもよい。

【００６８】

１１０４では、ランダムチャレンジがもはや有効ではないことを検出した時点で、安全なトランザクションサービス１０１は、新しいランダムチャレンジに対する要求をサーバ１３０に（図解される例では安全なトランザクションプラグイン１０５及びブラウザ１０４を介して）送信する。１１０５では、サーバ１３０は、新しいランダムチャレンジ、及びタイムアウト期間の新しい表示を生成する。一実施形態では、タイムアウト期間は、動作１１０１と同一であるか、又は修正され得る。例えば、サーバ１３０は、タイムアウト期間の継続時間を増加させて、クライアントとのデータトラフィックを減少させるか、又は継続時間を減少させて、ランダムチャレンジによって提供されたセキュリティのレベルを増加させることができる。１１０６では、新しいランダムチャレンジ及びタイムアウト表示は、安全なトランザクションサービス１０１に送信される。

【００６９】

残りのトランザクションが前述のように生じる。例えば、安全なトランザクションサービスは、図４、図１０Ｂ、又は図１０Ｃに関して上で論じられるようにデバイス登録及び鍵交換を実施するために、１１０７でサーバに直接安全な接続を開く。１１０８では、サーバ１３０は、ユーザを（例えば、ユーザ名又は他のＩＤで）識別し、認証デバイスを証明し、デバイスに対する鍵を生成する。述べられるように、鍵は、対称鍵又は非対称鍵で

あり得る。１１０９では、鍵は、安全な接続を介して安全なトランザクションサービス１０１に送信され、１１１０では、安全なトランザクションサービス１０１は、鍵を認証デバイスに登録する。１１１１では、登録が完了した通知がサーバ１３０に送信される。

【００７０】

したがって、図１１Ａに示される実施形態では、デバイス登録に使用される鍵は、図１０Ｂに示される実施形態のようにサーバ１３０で生成される。しかしながら、本発明の基本原理はまた、鍵（複数可）が図１０Ｃに関して上記に記載されるものなど、クライアント１００上の安全なトランザクションサービス１０１によって生成される実施形態で使用され得る。

【００７１】

図１１Ｂは、認証プロセスの文脈において実装される本発明の一実施形態を図解する。１１５１では、ユーザは、特定のウェブサイトのＵＲＬをブラウザ１０４に入力し、安全なトランザクションサーバ１３２～１３３を含むエンタープライズ／ウェブ宛先サーバ１３０内のウェブサーバ１３１に方向付けられる。１１５２では、クエリは、安全なトランザクションサービスに（ブラウザ及びプラグインを介して）送り返されて、どのデバイス（複数可）がウェブサイトのＵＲＬで登録されるかを決定する。安全なトランザクションサービス１０１は、クライアント１００上の安全なストレージ７２０に問い合わせて、１１５３でサーバ１３０に送り返されるデバイスのリストを識別する。１１５４では、サーバ１１５４は、認証のために使用するデバイスを選択し、ランダムチャレンジ及びタイムアウト表示を生成し、１１５５では、この情報を安全なトランザクションサービス１０１に送り返す。

【００７２】

１１５６では、安全なトランザクションサービス１１５６は、ランダムチャレンジがタイムアウト期間の終了に達する時点でもはや有効ではないことを自動的に検出する。上述のように、タイムアウト期間の終了を示し、検出するために様々な異なる技術が利用され得る（図１１Ａ及び関連したテキスト参照）。ランダムチャレンジの期限切れを検出した時点で、１１５７では、安全なトランザクションサービス１０１は、サーバ１３０に透過的に（即ち、ユーザが操作することなく）通知し、新しいランダムチャレンジを要求する。それに応答して、１１５８では、サーバ１３０は、新しいランダムチャレンジ、及びタイムアウト期間の新しい表示を生成する。述べられるように、新しいタイムアウト期間は、クライアントに以前に送信されたのと同一であり得るか、又は修正され得る。いずれの場合も、１１５９では、新しいランダムチャレンジ及びタイムアウト表示は、安全なトランザクションサービス１０１に送信される。

【００７３】

図１１Ｂに示される残りのトランザクション図は、上記に記載されるのと実質的に同一の様式で動作する（例えば、図５参照）。例えば、１１６０では、認証ユーザインターフェースが表示され（例えば、指紋センサ上で指をスワイプすることをユーザに指示して）、１１６１では、ユーザは認証を提供する（例えば、指紋スキャナ上で指をスワイプする）。１１６２では、安全なトランザクションサービスは、ユーザの身元を（例えば、ユーザから収集された認証データを安全なストレージ７２０内に記憶されたものと比較して）検証し、認証デバイスと関連付けられた鍵を使用して、ランダムチャレンジを暗号化する。１１６３では、ユーザ名（又は他のＩＤコード）及び暗号化されたランダムチャレンジは、サーバ１３０に送信される。最後に、１１６４では、サーバ１３０は、ユーザ名（又は他のＩＤコード）を用いて安全なトランザクションデータベース１２０内のユーザを識別し、安全なトランザクションデータベース１２０内に記憶された鍵を使用してランダムチャレンジを復号／検証して、認証プロセスを完了する。

【００７４】

認証フレームワーク内のプライバシークラスを実装するためのシステム及び方法

一実施形態では、複数のプライバシー保護のクラスは、エンドユーザによって事前に定義され、選択され、及び／又は修正され得る。プライバシークラスは、クライアントが公

表された情報を用いて識別され得る確率に基づいて定義され得る。比較的より高いプライバシーレベルを有するプライバシークラスでは、クライアントデバイスに関する比較的より少ない情報は、本明細書に記載される認証技術を実施するために公表される。一実施形態では、ユーザは、異なるサーバと通信するとき、最小限の情報を開示するために選択することができる（即ち、各ウェブサイト又はネットワークサービスに対して最低の許容可能なプライバシーインパクトを有するトランザクションを選択することができる）。

【００７５】

図１２は、プライバシークラスを実装するための高レベルのアーキテクチャを図解する。図解されるように、本実施形態の安全なトランザクションサービス１０１は、認証デバイスに関連する情報等のクライアント情報に対してサーバ１３０から受信されたクエリを分析し、このようなクエリに応答してプライバシーポリシーを実装し、かつ使用中の特定のプライバシークラスに基づいて収集されたクライアント情報を含む応答を生成するためのプライバシー管理論理１２０１を含む。一実施形態では、プライバシー管理モジュール１２０１は、安全なトランザクションサービス１０１の文脈において実行されたソフトウェアモジュールとして実装される。しかしながら、プライバシー管理モジュール１２０１は、本発明の基本原理に依然として適合しながら任意の様式で実装されてもよく、ソフトウェア、ハードウェア、ファームウェア、又はこれらの任意の組み合わせを含んでもよいことに留意されたい。

【００７６】

プライバシー管理論理１２０１によって利用されるプライバシークラスは、クライアント１００上に事前に指定され、記憶され（例えば、安全なストレージ７２０内に記憶された中に）得る。一実施形態では、高いプライバシーインパクト、中間プライバシーインパクト、及び低いプライバシーインパクトという３つのプライバシークラスが定義される。各プライバシークラスは、公表された情報がユーザ／クライアントを一意的に識別するために使用され得る確率に基づいて定義され得る。例えば、低いプライバシーインパクトのトランザクションに公表された情報は、１０％のユーザ又はマシンの確率がインターネット上で一意的に識別されることをもたらす場合があり、中間プライバシーインパクトのトランザクションは、５０％のユーザ又はマシンの確率が一意的に識別されることをもたらす場合があり、高いプライバシーインパクトのトランザクションは、１００％のユーザ又はマシンの確率が一意的に識別されることをもたらす場合がある。様々な他のプライバシークラスのレベルは、本発明の基本原理に依然として適合しながら定義され得る。

【００７７】

一実施形態では、各信頼パーティ（例えば、各ウェブサイト１３１又はサービス１５１）は、必要なプライバシークラス又は他のプライバシー閾値を指定することができる。例えば、高められたセキュリティのレベルを必要とするウェブサイト及びサービスは、高いプライバシーインパクトクラスに従った通信のみを可能にし得るが、一方、他のウェブサイト／サービスは、中間プライバシーインパクト又は低いプライバシーインパクトクラスを用いて対話を許可することができる。一実施形態では、サービス１３０から送信されたクライアント情報に関するクエリは、どの情報のプライバシークラスが取り出されるべきであるか（即ち、低、中、高）を指定する属性を含む。したがって、プライバシー管理論理１２０１は、各信頼パーティに対する最も承認されたプライバシークラスの情報を記憶する。一実施形態では、信頼パーティは、既に承認されたものより高いプライバシークラスに属する情報を要求するたびに、ユーザは、この信頼パーティに対してこの新しいプライバシークラスを永久に承認（又は拒否）するように指示される。ユーザの承認に応答して、プライバシー管理論理は、信頼パーティ（例えば、ＵＲＬを介して識別される）と新しいプライバシークラスとの間の新しい関連性を記憶することができる。

【００７８】

ユーザ選好１２３０は、単純化のために図１２におけるプライバシー管理論理に直接適用されるが、ユーザは、ブラウザベースのグラフィカルユーザインターフェース（図示せず）を介して選好を指定し得ることに留意されたい。このような場合、ユーザは、ブラウ

ザのウィンドウを介してプライバシー設定を入力する。安全なトランザクションプラグイン１０５は次に、プライバシー管理論理１２０１に、又はプライバシー管理論理１２０１によってアクセス可能な構成データファイルに新しい設定を記憶する。要するに、本発明の基本原理は、プライバシー管理論理を構成するための任意の特定の機構に限定されない。

【００７９】

様々なタイプのクライアントデータは、例えば、機械モデル識別子、クライアントソフトウェア情報、クライアント能力、及びクライアントデバイス上に構成された各認証デバイスに関連する様々なレベルの情報（例えば、デバイスＩＤコード、ベンダＩＤコード、デバイスクラスＩＤなど）を含む様々なプライバシークラスレベルで指定され得る。この情報の異なる組み合わせは、異なるプライバシークラスを定義する上記に指定された百分率を決定するために収集され得る。

【００８０】

図１３は、定義されたプライバシークラスを用いて要求当事者に情報を提供するための一連のトランザクションを図解する。１３０１では、サーバ１３０は、クライアントデバイス情報に関するクエリを含む通知を生成する。１３０２では、クエリは、クライアントに送信され、安全なトランザクションサービス１０１によって最終的に受信される。１３０３では、安全なトランザクションサービスのプライバシー管理論理は、応答に対するプライバシークラスを決定し、必要な情報を収集する。上述のように、Ｎ個の異なるプライバシークラスレベルが定義されてもよく、安全なトランザクションサービス１０１は、クライアントに関する最小限の情報を同時に公表しながら、要求当事者の要件に適合するものを選択することができる。１３０４では、収集された情報は、サーバ１３０に送信され、１３０５では、サーバは、クライアントとの１つ以上の後続のトランザクションに対する情報を使用する。

【００８１】

トランザクション署名を用いて認証フレームワークを実装するためのシステム及び方法

本発明の一実施形態は、トランザクション状態がクライアントとのセッションを維持するためにサーバ上に維持される必要がないように、安全なトランザクションサーバ上のトランザクション署名を利用する。具体的には、トランザクションテキスト等のトランザクション詳細は、サーバによって署名されたクライアントに送信され得る。サーバは次に、クライアントによって受信された署名されたトランザクション応答がシグネチャを検証することによって有効であることを検証することができる。サーバは、トランザクションコンテンツを持続的に記憶する必要はなく、これは、多数のクライアントのためのかなりの量のストレージ空間を消費し、サーバ上にサービス妨害タイプの攻撃の可能性を開く。

【００８２】

本発明の一実施形態は、クライアント１００とトランザクションを開始するウェブサイト又は他のネットワークサービス（１４０１）を示す図１４に図解される。例えば、ユーザは、ウェブサイト上に購入のための選択された品目を有してもよく、チェックアウト及び支払いをする準備ができていてもよい。図解される例では、ウェブサイト又はサービス１４０１は、シグネチャ（本明細書に記載されるような）を生成及び検証するためのシグネチャ処理論理１４０３と、クライアント認証１４０４を実施する（例えば、前述の認証技術を用いて）ための認証論理とを含む、安全なトランザクションサーバ１４０２にトランザクションを渡す。

【００８３】

一実施形態では、安全なトランザクションサーバ１４０２からクライアント１００に送信された認証要求は、暗号ノンス（上記に記載されるような）などのランダムチャレンジ、トランザクション詳細（例えば、トランザクションを完了するために提示された特定のテキスト）、並びに秘密鍵（安全なトランザクションサーバによってのみ知られる）を用いてランダムチャレンジ及びトランザクション詳細上でシグネチャ処理論理１４０３によって生成されたシグネチャを含む。

【００８４】
上記の情報がクライアントによって受信されると、ユーザは、トランザクションを完了するために認証が必要とされる表示を受信することができる。それに応答して、ユーザは、例えば、指紋スキャナにわたって指をスワイプするか、スナップ写真を撮るか、マイクロホンに向かって話すか、又は所定のトランザクションに許可される任意の他のタイプの認証を実施することができる。一実施形態では、ユーザがクライアント１００上の認証に成功すると、クライアントは、サーバに以下を送り返す：（１）ランダムチャレンジ及びトランザクションテキスト（両方ともサーバによってクライアントに以前に提供される）、（２）ユーザが認証の完了に成功したことを証明する認証データ、及び（３）シグネチャ。

【００８５】
安全なトランザクションサーバ１４０２上の認証モジュール１４０４は次に、ユーザが現在認証されていることを確認することができ、シグネチャ処理論理１４０３は、秘密鍵を使用してランダムチャレンジ及びトランザクションテキスト上にシグネチャを再生する。シグネチャがクライアントによって送信されたものと一致する場合、サーバは、トランザクションテキストがウェブサイト又はサービス１４０１から最初に受信されたのと同一であることを検証することができる。安全なトランザクションサーバ１４０２が安全なトランザクションデータベース１２０内にトランザクションテキスト（又は他のトランザクションデータ）を持続的に記憶することを必要とされないため、ストレージリソース及び処理リソースが節約される。

【００８６】
例示的なデータ処理デバイス
図１５は、本発明のいくつかの実施形態に使用され得る例示的なクライアント及びサーバを図解するブロック図である。図１５は、コンピュータシステムの様々な構成要素を図解するが、このような詳細が本発明に密接な関係がないように構成要素を相互接続する任意の特定のアーキテクチャ又は様式を表すことを意図しないことが理解されるべきである。より少ない構成要素又はより多くの構成要素を有する他のコンピュータシステムもまた、本発明と共に使用され得ることが理解されるであろう。

【００８７】
図１５に図解されるように、データ処理システムの形態であるコンピュータシステム１５００は、処理システム１５２０、電源１５２５、メモリ１５３０、及び不揮発性メモリ１５４０（例えば、ハードドライブ、フラッシュメモリ、相変化メモリ（ＰＣＭ）など）と連結されるバス（複数可）１５５０を含む。バス（複数可）１５５０は、当該技術分野において周知であるように様々なブリッジ、コントローラ、及び／又はアダプタを通じて互いに接続され得る。処理システム１５２０は、メモリ１５３０及び／又は不揮発性メモリ１５４０から命令（複数可）を取り出し、上記に記載されるような動作を実施する命令を実行することができる。バス１５５０は、上記の構成要素を共に相互接続し、同様に、これらの構成要素を、任意のドック１５６０、表示コントローラ＆表示デバイス１５７０、入力／出力デバイス１５８０（例えば、ＮＩＣ（ネットワークインターフェースカード）、カーソル制御（例えば、マウス、タッチスクリーン、タッチパッドなど）、キーボードなど）、並びに任意の無線送受信器（複数可）１５９０（例えば、Ｂｌｕｅｔｏｏｔｈ（登録商標）、ＷｉＦｉ、赤外線など）に相互接続する。

【００８８】
図１６は、本発明のいくつかの実施形態に使用され得る例示的なデータ処理システムを図解するブロック図である。例えば、データ処理システム１６００は、ハンドヘルドコンピュータ、携帯情報端末（ＰＤＡ）、携帯電話、携帯用ゲーミングシステム、携帯用メディアプレーヤ、タブレット、又は携帯電話、メディアプレーヤ、及び／若しくはゲーミングシステムを含み得るハンドヘルドコンピューティングデバイスであり得る。別の例として、データ処理システム１６００は、ネットワークコンピュータ、又は別のデバイス内の埋め込まれた処理デバイスであり得る。

【００８９】
本発明の一実施形態によれば、データ処理システム１６００の例示的なアーキテクチャは、上記に記載されるモバイルデバイスに使用され得る。データ処理システム１６００は、処理システム１６２０を含み、これは、集積回路上に１つ以上のマイクロプロセッサ及び／又はシステムを含むことができる。処理システム１６２０は、メモリ１６１０、電源１６２５（１つ以上のバッテリを含む）、音声入力／出力１６４０、表示コントローラ及び表示デバイス１６６０、任意の入力／出力１６５０、入力デバイス（複数可）１６７０、並びに無線送受信器（複数可）１６３０と連結される。図１６に示されない追加の構成要素もまた、本発明のある特定の実施形態においてデータ処理システム１６００の一部であり得、本発明のある特定の実施形態において、図１６に示されるより少ない構成要素が使用され得ることが理解されるであろう。加えて、図１６に示されない１つ以上のバスが当該技術分野において周知であるような様々な構成要素を相互接続するために使用され得ることが理解されるであろう。
【００９０】
メモリ１６１０は、データ処理システム１６００による実行のためにデータ及び／又はプログラムを記憶することができる。音声入力／出力１６４０は、例えば、音楽を再生し、及び／又はスピーカ及びマイクロホンを通じて電話機能を提供するマイクロホン及び／又はスピーカを含むことができる。表示コントローラ及び表示デバイス１６６０は、グラフィカルユーザインターフェース（ＧＵＩ）を含むことができる。無線（例えば、ＲＦ）送受信器１６３０（例えば、ＷｉＦｉ送受信器、赤外線送受信器、Ｂｌｕｅｔｏｏｔｈ（登録商標）送受信器、無線セルラー電話送受信器など）は、他のデータ処理システムと通信するために使用され得る。１つ以上の入力デバイス１６７０により、ユーザはシステムに入力を提供することができる。これらの入力デバイスは、キーパッド、キーボード、タッチパネル、マルチタッチパネルなどであり得る。任意の他の入力／出力１６５０は、ドックのためのコネクタであり得る。
【００９１】
本発明の実施形態は、上記に記載されるような様々なステップを含むことができる。ステップは、汎用又は特殊用途プロセッサにある特定のステップを実施させる機械実行可能な命令に具現化することができる。あるいは、これらのステップは、ステップを実施するための配線論理を含む特定のハードウェア構成要素によって、又はプログラムされたコンピュータ構成要素とカスタムハードウェア構成要素との任意の組み合わせによって実施され得る。
【００９２】
本発明の要素はまた、機械実行可能なプログラムコードを記憶するために機械可読媒体として提供され得る。機械可読媒体は、これらに限定されないが、フロッピー（登録商標）ディスケット、光ディスク、ＣＤ－ＲＯＭ、及び光磁気ディスク、ＲＯＭ、ＲＡＭ、ＥＰＲＯＭ、ＥＥＰＲＯＭ、磁気カード若しくは光カード、又は電子プログラムコードを記憶するのに好適な他のタイプの媒体／機械可読媒体を含むことができる。
【００９３】
前述の説明全体を通して、説明のために、本発明の十分な理解を提供するために数多くの特定の詳細が記載された。しかしながら、本発明は、これらの特定の詳細のうちのいくつかを用いることなく実践され得ることが当業者に明らかであろう。例えば、本明細書に記載される機能モジュール及び方法は、ソフトウェア、ハードウェア、又はこれらの任意の組み合わせとして実装され得ることが当業者に容易に明らかであろう。更に、本発明のいくつかの実施形態がモバイルコンピューティング環境の文脈において本明細書に記載されるが、本発明の基本原理は、モバイルコンピューティング実装形態に限定されない。事実上あらゆるタイプのクライアント又はピアデータ処理デバイスが、例えば、デスクトップ又はワークステーションコンピュータを含むいくつかの実施形態で使用され得る。したがって、本発明の範囲及び趣旨は、以下の特許請求の範囲において判断されるべきである。

なお、上記開示事項に加えて、原出願の特許請求の範囲に記載された事項を更に開示する。

〔事項１〕

方法であって、

許容できる認証能力のセットを識別するポリシーを受信する工程と、

クライアント認証能力のセットを決定する工程と、

前記決定されたクライアント認証能力のセットに基づいて前記許容できる認証能力のセットをフィルタリングして、前記クライアントのユーザを認証するためのフィルタリングされた１つ以上の認証能力のセットを導出する工程と、

前記フィルタリングされた１つ以上の認証能力のセットを使用して、ネットワーク上で前記ユーザを認証する工程と、を含む、方法。

〔事項２〕

前記クライアント上の安全なストレージから読み取ることによって前記クライアント認証能力のセットを決定する工程を更に含む、事項１に記載の方法。

〔事項３〕

前記ポリシーが、ネットワークサーバによって許容できると見なされる認証デバイスタイプ及び／又はクラスのセットを含む、事項１に記載の方法。

〔事項４〕

前記フィルタリングされた認証能力のセットのうちの１つ以上をグラフィカルユーザインターフェース（ＧＵＩ）に表示する工程と、

前記リストから認証能力のうちの１つ以上を選択又は優先順位付けすることをユーザに問い合わせる工程と、

前記クエリへのユーザ入力に基づいて、認証能力のフィルタリングされたユーザ指定のリストを生成する工程と、を更に含む、事項１に記載の方法。

〔事項５〕

前記認証能力が、指紋センサを含む、事項１に記載の方法。

〔事項６〕

前記認証能力が、音声認証能力を含む、事項１に記載の方法。

〔事項７〕

前記認証能力が、スマートカードを含む、事項１に記載の方法。

〔事項８〕

前記認証能力が、トラステッドプラットフォームモジュール（ＴＰＭ）を含む、事項１に記載の方法。

〔事項９〕

方法であって、

Ｎ＞１である、クライアント上のＮ個の認証デバイスを検出する工程と、

前記Ｎ個の認証デバイスの各々に１つずつ、Ｎ個の暗号エンティティを生成する工程と、

前記Ｎ個の暗号エンティティの各々を前記Ｎ個の認証デバイスの各々に登録するコマンドを前記クライアントに送信する工程と、

前記クライアント上で前記コマンドを実行し、それに応答して前記Ｎ個の暗号エンティティの各々を前記それぞれのＮ個の認証デバイスの各々に登録する工程と、

その後、前記認証デバイスのうちの少なくとも１つ及びその関連付けられた暗号エンティティを使用して、ネットワーク上で前記クライアントのユーザを認証する工程と、を含む、方法。

〔事項１０〕

暗号エンティティが、鍵を含む、事項９に記載の方法。

〔事項１１〕

前記鍵が、対称鍵を含み、所定の鍵の同一のコピーが、前記クライアント上の安全なストレージ、及びサーバと関連付けられた安全なストレージ内に記憶される、事項１０に記

載の方法。
〔事項１２〕
前記鍵が、非対称鍵対を含み、前記鍵対の第１の鍵が、前記クライアント上の安全なストレージ内に記憶され、前記鍵対の第２の鍵が、サーバと関連付けられた安全なストレージ内に記憶される、事項１０に記載の方法。
〔事項１３〕
ユーザを認証するために前記認証デバイスのうちの少なくとも１つ及びその関連付けられた暗号エンティティを使用する工程が、
前記認証デバイスから生体ユーザ入力を受信する工程と、
前記生体ユーザ入力が前記ユーザの認証に成功したことを決定する工程と、
前記認証デバイスと関連付けられた前記暗号エンティティを使用して、サーバに送信される情報を暗号化する工程と、を含む、事項９に記載の方法。
〔事項１４〕
前記Ｎ個の認証デバイスの全てが登録されたという通知を前記サーバに送信する工程を更に含む、事項９に記載の方法。
〔事項１５〕
前記サーバから前記クライアントにランダムチャレンジを最初に送信する工程と、
前記Ｎ個の認証デバイスの全てが登録されたという通知と共に、前記ランダムチャレンジを前記サーバに送り返す工程と、を更に含み、
前記サーバが、受信された前記ランダムチャレンジが送信された前記ランダムチャレンジと同一であるかを検証する、事項１４に記載の方法。
〔事項１６〕
前記サーバが、特定の認証デバイスと関連付けられた暗号エンティティを使用して、前記クライアント及び／又は前記認証デバイスの身元を検証する、事項９に記載の方法。
〔事項１７〕
前記鍵が、鍵プロビジョニングプロトコルを用いて送信される、事項９に記載の方法。
〔事項１８〕
前記プロビジョニングプロトコルが、動的対称鍵プロビジョニングプロトコル（ＳＤＫＰＰ）を含む、事項１７に記載の方法。
〔事項１９〕
方法であって、
前記クライアントに通信可能に連結された認証デバイスを用いてネットワーク登録又は認証プロセスの文脈において、ランダムチャレンジ及び前記ランダムチャレンジと関連付けられたタイムアウト期間の表示をサーバからクライアントに送信する工程と、
前記タイムアウト期間に基づいて、前記ランダムチャレンジがもはや有効ではないことを自動的に検出する工程と、
それに応答して、前記クライアントからサーバに新しいランダムチャレンジに対する要求を送信する工程と、を含み、送信する工程が、前記クライアントのユーザに透過的に実施される、方法。
〔事項２０〕
前記ランダムチャレンジが、前記サーバから生成された乱数又はランダムＩＤコードを含む、事項１９に記載の方法。
〔事項２１〕
前記ランダムチャレンジが、暗号ノンスを含む、事項２０に記載の方法。
〔事項２２〕
前記クライアントから前記サーバに前記ランダムチャレンジを送信して、前記クライアントと前記サーバとの間に安全な接続を確立する工程を更に含む、事項１９に記載の方法。
〔事項２３〕
前記サーバから前記新を受信する工程と、

前記クライアントから前記サーバに前記ランダムチャレンジを送信して、前記クライアントと前記サーバとの間に安全な接続を確立する工程と、を更に含む、事項１９に記載の方法。

〔事項２４〕

ユーザから生体認証データを収集する工程と、

前記新しいランダムチャレンジが前記期間の期限切れにより無効になる前に、前記生体認証データを用いて前記ユーザの身元を確認する工程と、

前記新しいランダムチャレンジと共に前記新しい認証データを前記サーバに送信する工程と、を更に含む、事項１９に記載の方法。

〔事項２５〕

前記サーバが、前記ユーザの身元を検証し、前記ランダムチャレンジを復号する、事項２４に記載の方法。

〔事項２６〕

前記タイムアウト期間の前記表示が、前記ランダムチャレンジが無効になった後の時間量を含む、事項１９に記載の方法。

〔事項２７〕

前記タイムアウト期間の前記表示が、前記サーバから前記クライアントへの前記ランダムチャレンジの前記送信と関連付けられたタイムスタンプを含む、事項２６に記載の方法。

〔事項２８〕

前記タイムアウト期間の前記表示が、特定の時間を含む、事項１９に記載の方法。

〔事項２９〕

方法であって、

クライアント情報に関するクエリをサーバからクライアントに送信する工程であって、前記クライアント情報が、前記クライアントに連結された認証デバイスに関連する情報を含む、工程と、

前記クエリを分析して、前記サーバにクライアント情報を提供するために使用される適切なプライバシークラスを決定する工程と、

前記決定されたプライバシークラスに基づいて選択されるクライアント情報のサブセットを提供する工程であって、前記クライアント情報のサブセットが、前記クライアントに連結された前記認証デバイスに関連する前記情報を含む、工程と、

認証フレームワーク内の前記クライアント情報のサブセットを使用して、ネットワーク上でユーザ認証サービスを提供する工程と、を含む、方法。

〔事項３０〕

前記プライバシークラスが、第１のプライバシーレベルを提供する第１のプライバシークラス、第２のプライバシーレベルを提供する第２のプライバシークラス、及び第３のプライバシーレベルを提供する第３のプライバシークラスからなる群から選択される、事項２９に記載の方法。

〔事項３１〕

各プライバシークラスが、前記クライアントを識別するのに使用可能なクライアント情報及び／又は認証デバイス情報の異なるセットを指定する、事項２９に記載の方法。

〔事項３２〕

各プライバシークラスが、クライアントがそのプライバシークラスによって明らかにされた前記クライアント情報及び／又は認証デバイス情報を用いて識別され得る確率に基づいて定義される、事項３１に記載の方法。

〔事項３３〕

前記サーバから送信されたクライアント情報に関する前記クエリが、取り出される必要がある情報の前記プライバシークラスを指定する属性を含む、事項２９に記載の方法。

〔事項３４〕

別個のプライバシークラスが、各信頼パーティに対して選択される、事項２９に記載の

方法。
〔事項３５〕
安全なストレージ内の各信頼パーティに対して最も承認されたプライバシークラスのための情報を関連付ける工程を更に含む、事項３４に記載の方法。
〔事項３６〕
前記信頼パーティが前記信頼パーティと既に関連付けられたプライバシークラスより高いプライバシークラスに属する情報を要求するたびに、前記ユーザが、この信頼パーティに対してこの新しいプライバシークラスを永久に承認又は拒否するように指示される、事項３５に記載の方法。
〔事項３７〕
前記プライバシークラスに基づいて選択される前記情報のサブセットが、機械モデル識別子（ＭＭＩＤ）、クライアントソフトウェア情報、クライアント能力、及び前記クライアントデバイス上で構成された各認証デバイスに関連する情報のうちの１つ以上を含む、事項２９に記載の方法。
〔事項３８〕
各認証デバイスに関連する前記情報が、デバイスＩＤコード、ベンダＩＤコード、及びデバイスクラスＩＤのうちの１つ以上を含む、事項３７に記載の方法。
〔事項３９〕
前記サーバが、前記クライアントとの１つ以上の後続のトランザクションに対して前記クライアント情報のサブセットを使用する、事項２９に記載の方法。
〔事項４０〕
前記１つ以上の後続のトランザクションが、ネットワーク上でユーザを認証する工程を含む、事項３９に記載の方法。
〔事項４１〕
方法であって、
第１のサーバとクライアントとの間のオンライントランザクションを実行する工程と、
前記オンライントランザクションのトランザクション詳細を第２のサーバに提供する工程と、
前記第２のサーバで鍵を使用して前記トランザクション詳細上にシグネチャを生成する工程と、
前記シグネチャ及び前記トランザクション詳細と共に前記クライアントに認証要求を送信する工程と、
前記クライアント上のユーザを認証して、認証データを生成する工程であって、前記認証データが、前記ユーザが前記クライアント上で認証に成功したかを指定する、工程と、
前記認証データ、前記トランザクション詳細、及び前記シグネチャを前記第２のサーバに送信する工程と、
前記トランザクション詳細及び前記鍵を使用して、前記シグネチャの有効性を確認する工程と、前記認証詳細を使用して、前記第２のサーバで前記クライアントを認証する工程と、を含み、前記シグネチャの有効性を確認し、かつ前記クライアントを認証した時点で、前記第２のサーバが、前記トランザクションについての確認を前記第１のサーバに送信する、方法。
〔事項４２〕
前記確認を受信した時点で、前記第１のサーバが、前記トランザクションを完了する、事項４１に記載の方法。
〔事項４３〕
前記トランザクション詳細が、トランザクションテキストを含む、事項４１に記載の方法。
〔事項４４〕
前記第２のサーバでランダムチャレンジを生成する工程と、
前記第２のサーバで前記鍵を使用して前記トランザクション詳細及び前記ランダムチャ

レンジの両方の上で前記シグネチャを生成する工程と、を更に含む、事項４１に記載の方法。

〔事項４５〕

前記認証データ、前記トランザクション詳細、及び前記シグネチャと共に前記ランダムチャレンジを前記第２のサーバに送信する工程と、

前記トランザクション詳細、前記ランダムチャレンジ、及び前記鍵を使用して、前記シグネチャの有効性を確認する工程と、前記認証詳細を使用して、前記第２のサーバで前記クライアントを認証する工程と、を更に含む、事項４４に記載の方法。

〔事項４６〕

前記トランザクション詳細、前記ランダムチャレンジ、及び前記鍵を使用して、前記シグネチャの有効性を確認する工程が、前記トランザクション詳細及び前記ランダムチャレンジ上で暗号アルゴリズムを実行する工程を含み、前記鍵が、前記シグネチャを生成するために前記暗号アルゴリズムのシードとして使用される、事項４５に記載の方法。

〔事項４７〕

前記クライアント上で前記ユーザを認証する工程が、生体ハードウェア及び／又はソフトウェアを使用して前記ユーザを認証する工程を含む、事項４０に記載の方法。

〔事項４８〕

前記生体ハードウェアが、指紋センサを備え、前記認証データが、前記ユーザの指がエンロールされた指紋と一致するかを示す、事項４７に記載の方法。

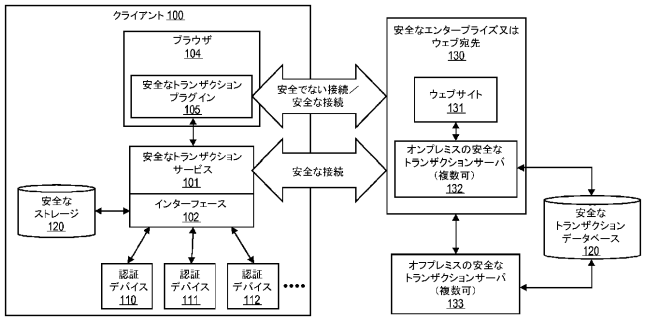
〔事項４９〕

前記生体ハードウェア及び／又はソフトウェアが、音声認識ハードウェア及び／又はソフトウェアを備え、前記認証データが、前記ユーザの声がエンロールされた声と一致するかを示す、事項４７に記載の方法。

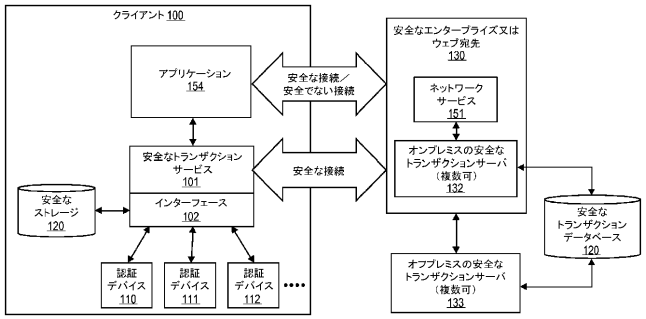
〔事項５０〕

前記第１のサーバが、前記クライアントにインストールされたウェブブラウザを介してアクセス可能なウェブサーバを備える、事項４１に記載の方法。

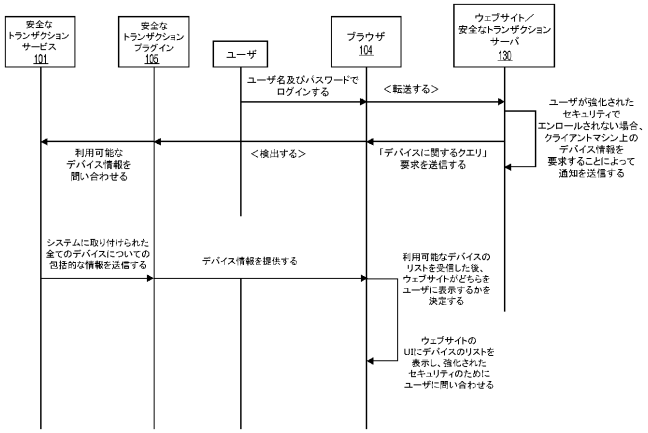
【図１Ａ】



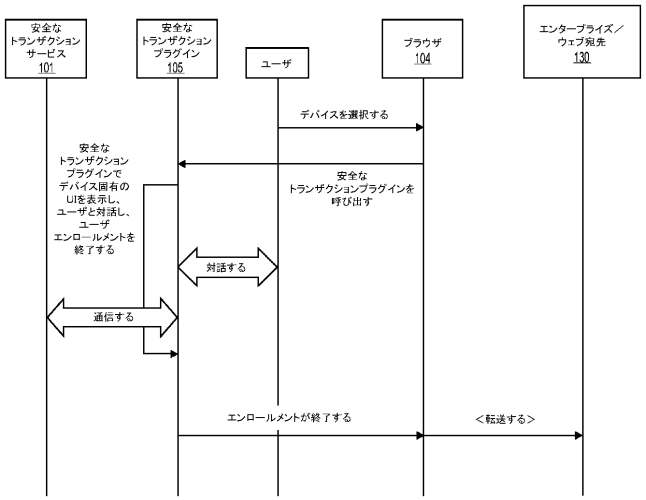
【図１Ｂ】



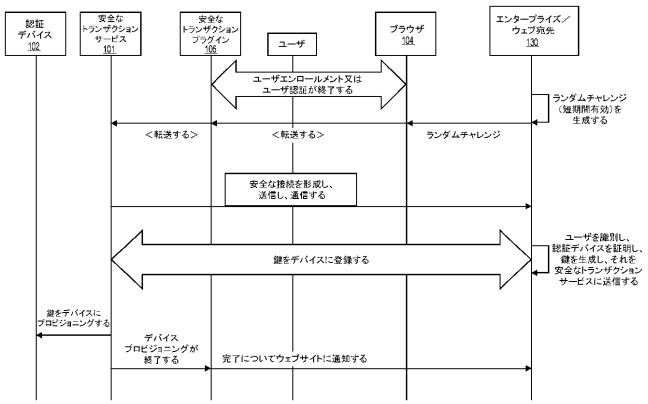
【図２】



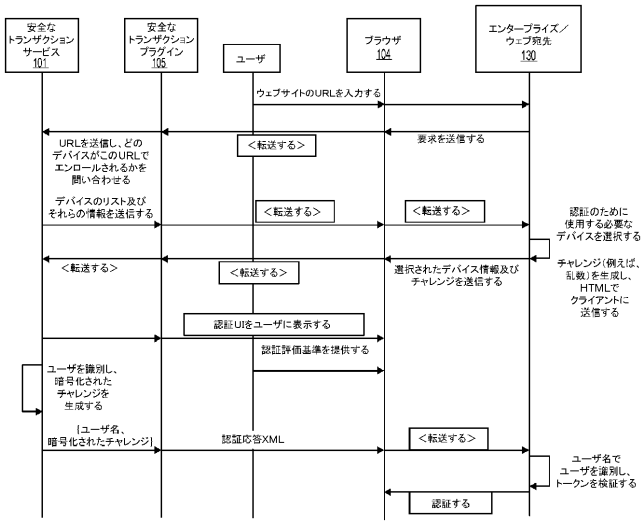
【図３】



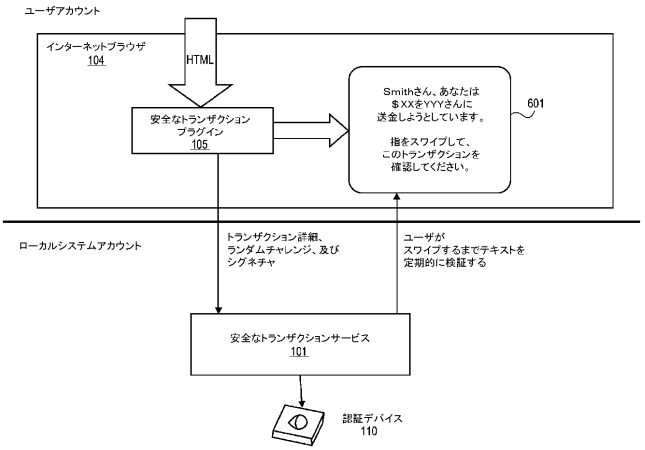
【図４】



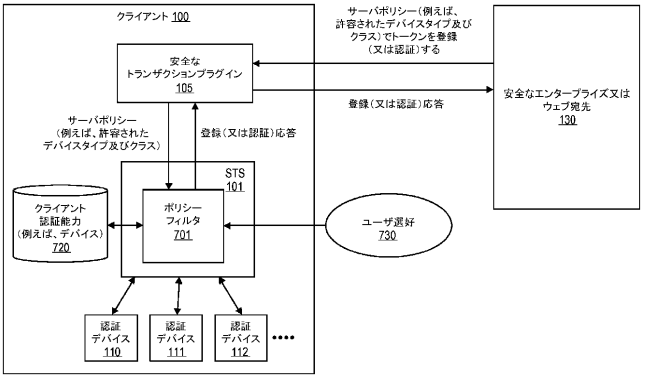
【図５】



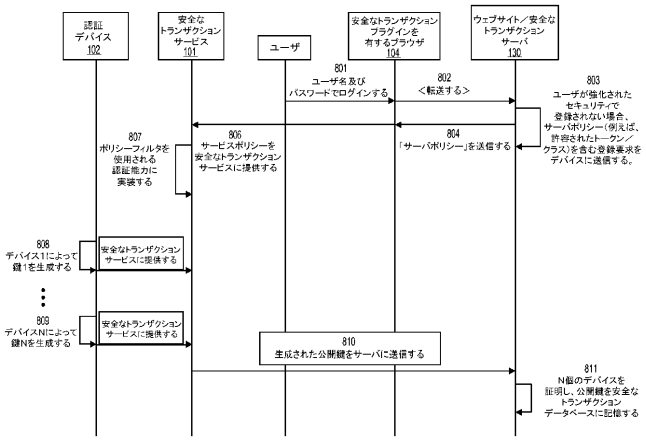
【図６】



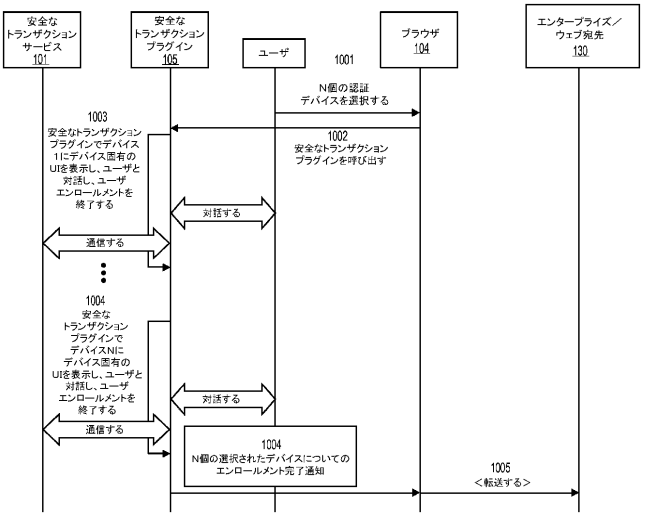
【図７】



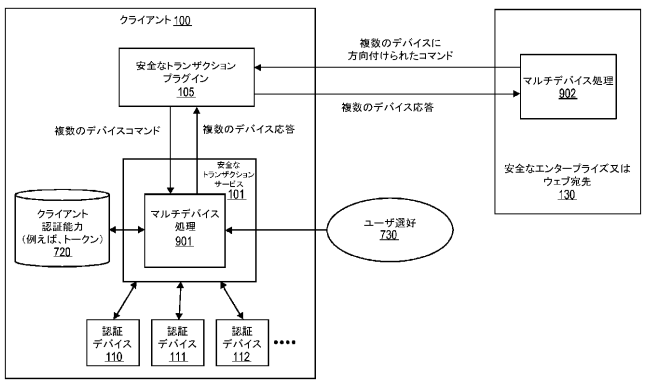
【図８】



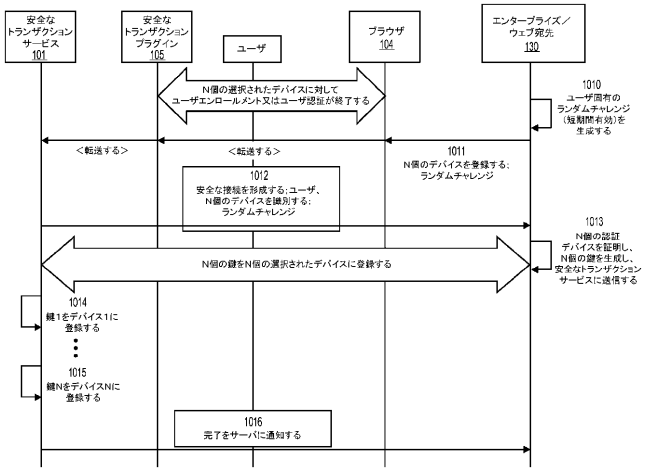
【図１０Ａ】



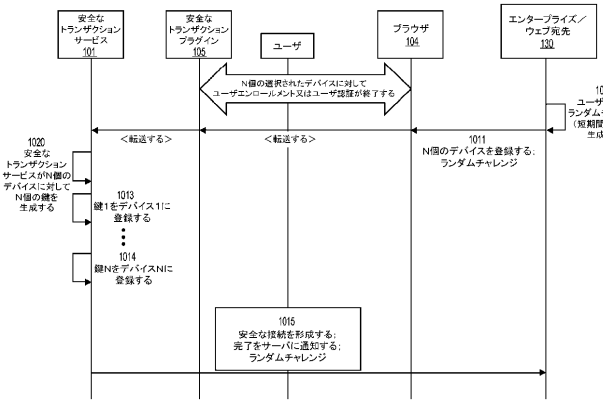
【図９】



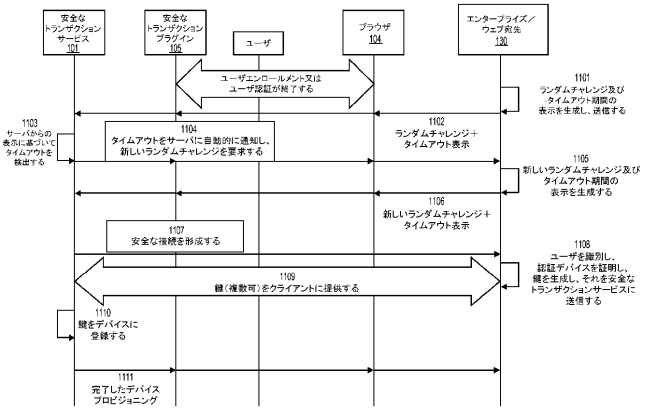
【図１０Ｂ】



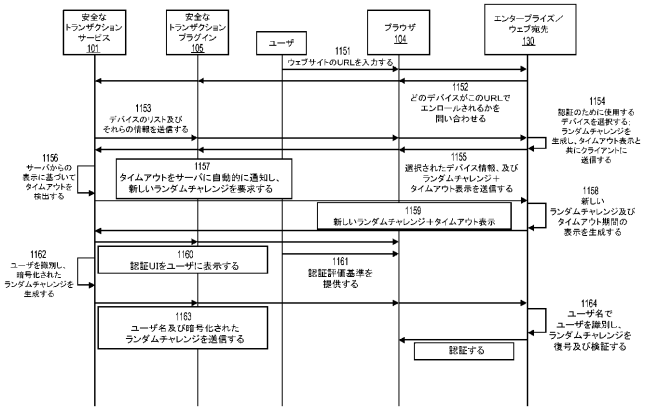
【図１０Ｃ】



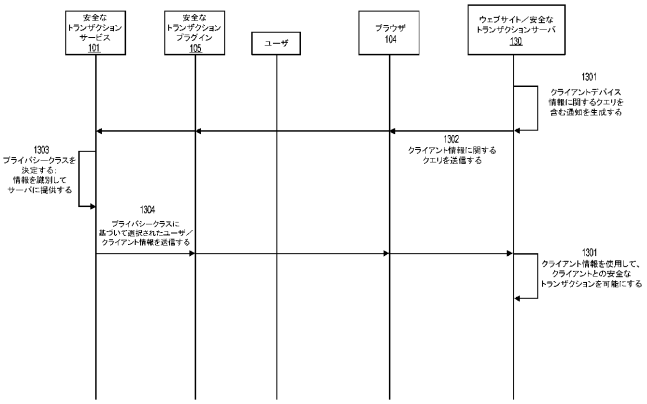
【図１１Ａ】



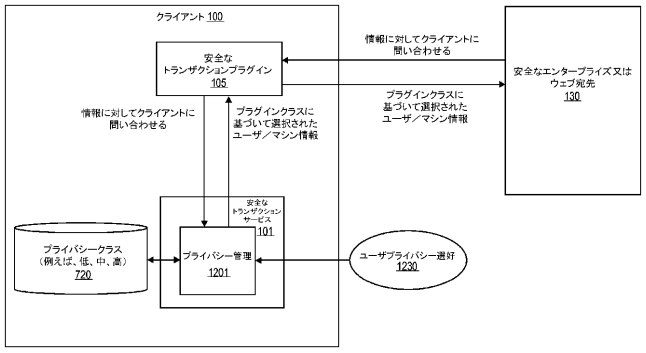
【図１１Ｂ】



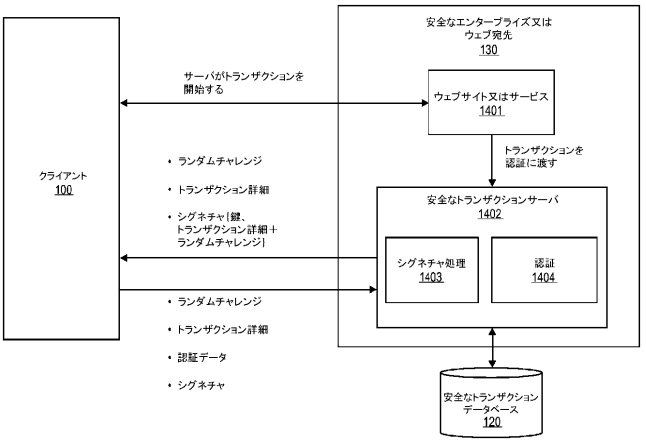
【図１３】



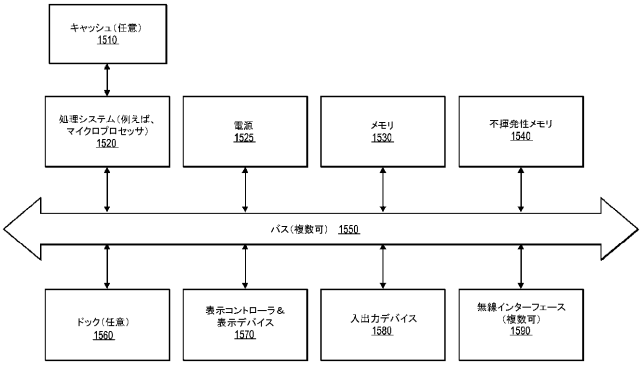
【図１２】



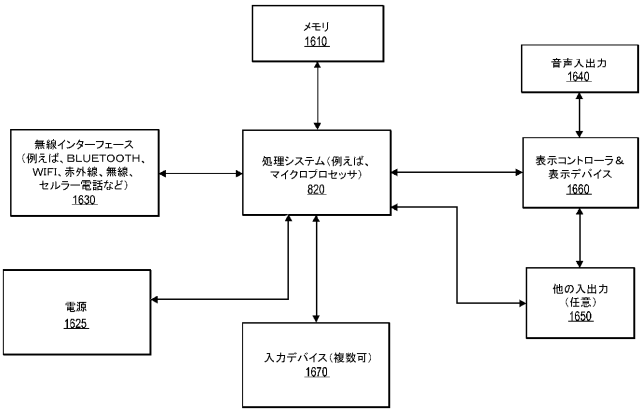
【図１４】



【図１５】


キャッシュ（任意）
1510
処理システム（例えば、
マイクロプロセッサ）
1520
電源
1525
メモリ
1530
不揮発性メモリ
1540
バス（複数可） 1550
ドック（任意）
1560
表示コントローラ＆
表示デバイス
1570
入出力デバイス
1580
無線インターフェース
（複数可）
1590

【図１６】


メモリ
1610
音声入出力
1640
無線インターフェース
（例えば、BLUETOOTH、
WIFI、赤外線、無線、
セルラー電話など）
1630
処理システム（例えば、
マイクロプロセッサ）
820
表示コントローラ＆
表示デバイス
1660
電源
1525
他の入出力
（任意）
1650
入力デバイス（複数可）
1670

フロントページの続き

(31)優先権主張番号 13/730,791
(32)優先日 平成24年12月28日(2012.12.28)
(33)優先権主張国 米国(US)
(31)優先権主張番号 13/730,795
(32)優先日 平成24年12月28日(2012.12.28)
(33)優先権主張国 米国(US)

(74)代理人 100082005
弁理士 熊倉 禎男
(74)代理人 100067013
弁理士 大塚 文昭
(74)代理人 100086771
弁理士 西島 孝喜
(74)代理人 100109070
弁理士 須田 洋之
(74)代理人 100109335
弁理士 上杉 浩
(74)代理人 100120525
弁理士 近藤 直樹
(72)発明者 バグダサリアン ダヴィット
アメリカ合衆国 カリフォルニア州 ９４３０３ パロ アルト ミドルフィールド ロード ４１５１ スイート ２００
(72)発明者 ローリー マット
アメリカ合衆国 カリフォルニア州 ９４３０３ パロ アルト ミドルフィールド ロード ４１５１ スイート ２００
(72)発明者 リンデマン ロルフ
アメリカ合衆国 カリフォルニア州 ９４３０３ パロ アルト ミドルフィールド ロード ４１５１ スイート ２００
(72)発明者 ウィルソン ブレンドン ジェイ
アメリカ合衆国 カリフォルニア州 ９４３０３ パロ アルト ミドルフィールド ロード ４１５１ スイート ２００
(72)発明者 ブリセノ マーク
アメリカ合衆国 カリフォルニア州 ９４３０３ パロ アルト ミドルフィールド ロード ４１５１ スイート ２００
(72)発明者 ドラキア ラジーヴ
アメリカ合衆国 カリフォルニア州 ９４３０３ パロ アルト ミドルフィールド ロード ４１５１ スイート ２００
(72)発明者 ナガラジャン ナガ
アメリカ合衆国 カリフォルニア州 ９４３０３ パロ アルト ミドルフィールド ロード ４１５１ スイート ２００

Ｆターム(参考) 5J104 AA07 AA16 AA32 AA36 DA03 EA04 EA18 EA19 JA03 JA21
KA01 KA04 KA05 KA06 NA02 NA36 NA37 NA38 PA07